Trevance® User Guide

Auric Systems International
Payment Processing Simplified™

19 August 2013

Version 3.0

Copyright © 1994-2013 Auric Systems International. All rights reserved.

Contents

1 Welcome **1**
- 1.1 PCI Compliance . . . 3
- 1.2 Passwords . . . 3
- 1.3 Access to the Underlying Operating System . . . 4
- 1.4 Encrypting Sensitive Data . . . 4
- 1.5 Submitting Transactions through the Web . . . 4
- 1.6 Contacting Auric Systems International . . . 4

I Installation and Configuration **7**

2 Installing Trevance® **9**
- 2.1 Minimum and Recommended System Requirements . . . 9
  - 2.1.1 Minimum System Requirements . . . 9
  - 2.1.2 Recommended System Requirements . . . 9
  - 2.1.3 Important Information . . . 10
- 2.2 Installing Trevance® . . . 10
  - 2.2.1 Installation Options . . . 10
  - 2.2.2 Installation Procedure . . . 11
- 2.3 Starting Trevance® the First Time . . . 15
- 2.4 Creating a New Administrator (and Web User) . . . 17
  - 2.4.1 Creating a New Administrator . . . 18
  - 2.4.2 Deleting the Default ADMIN User . . . 19
  - 2.4.3 Creating a New Web User . . . 20
  - 2.4.4 Deleting the Default WEB User . . . 22

3 Configuring Trevance® **23**
- 3.1 Preparing for Configuration . . . 24
  - 3.1.1 Using the Demonstration Version and Running Trevance® As an Application . . . 24
  - 3.1.2 Running the Trevance® Console and Server on the Same Machines . . . 25
  - 3.1.3 Pausing Trevance® . . . 25
  - 3.1.4 Checking the File Extension . . . 25
  - 3.1.5 Understanding Fields . . . 28

3.1.6 Restarting the Console When It Times Out 29
3.1.7 Saving Configuration Information 29
3.1.8 Configuring Currencies 30
3.2 Adding, Deleting, and Administering Users . . . 30
3.2.1 Adding a User 30
3.2.2 Changing User Information 33
3.2.3 Deleting a User 35
3.3 Configuring Processor Settings 36
3.3.1 Configuring Imports for Batch Files . . . 36
3.4 Configuring Exports for Batch Files 43
3.5 Generate Server Passphrase and Batch File Encryption Key 48
3.5.1 Generate Server Passphrase 48
3.5.2 Generate, Import, or Export an Encryption Key 50
3.6 Configuring the Real-Time Web Interface 54
3.6.1 Enable Web Interface and Change Server Port 55
3.6.2 Formatting the Web Request 56
3.6.3 Formatting the Web Response 62
3.7 Configuring Directories 66
3.7.1 Browsing (for local configuration only) . 67
3.7.2 Over-typing (for either local or remote configuration) 68
3.7.3 Returning to Defaults 69
3.8 Configuring Options 69
3.8.1 Changing General Options 70
3.8.2 Selecting a Secure File Deletion Method . 71
3.8.3 Changing File Extensions 72
3.8.4 Changing Troubleshooting Options 73
3.9 Producing a Configuration Report 75
3.10 Switching between Versions in Demo Mode . . . 80
3.11 Working with an Import File That Isn't Typical 81

4 Windows® Service 83
4.1 Establishing a Log-On Account for the Service . 83
4.1.1 All Directories Local 83
4.1.2 At Least One Remote Directory 84

4.1.3 After Establishing the Log-On Account . 85
4.2 Setting Up and Changing Remote Directories . . 85
4.2.1 Testing the Service 87

5 Testing and Activating Trevance® 89
5.1 Testing Your Configuration in Demo Mode . . . 89
5.1.1 Testing Your Batch Import and Export Configuration 89
5.1.2 Testing the Web Interface 93
5.2 Entering Your Serial Number and Activation Key 95
5.2.1 Switching from Demo Mode to Test Mode for the First Time 96
5.2.2 Switching between Modes 97
5.3 Testing Your Configuration in Test Mode 98

6 Understanding Trevance® 101
6.1 What Does Trevance® Do? 101
6.1.1 Batch Transactions 102
6.2 Understanding Delimited Text Files 107
6.3 Understanding Trevance® Terms 107
6.3.1 Done files 110
6.3.2 Export file and directory 110
6.4 Understanding the Trevance® Screen 114

7 Operation 119
7.1 Pausing, Resuming, Exiting, Launching the Console 119
7.1.1 Pausing or Resuming 119
7.1.2 Exiting and Launching as an Application 120
7.1.3 Launching the Console from the User Interface 120
7.2 Shutting Down and Restarting the Server 121
7.2.1 When Trevance® Is an Application . . . 122
7.2.2 When Trevance® Is a Service 122
7.3 Changing the Log, Batch, and Monitor Screens . 123
7.3.1 Changing the Width of Columns 123
7.3.2 Sorting Information 123
7.4 Understanding the Events Log 123

7.4.1 The Log Screen 124
7.4.2 The Log Files 125
7.5 Tracking Recent Batches 125
7.6 Using the Batch Submittal Queue 127
7.6.1 Viewing the Submittal Queue 127
7.6.2 Removing a Batch 129
7.6.3 Resending a Batch 131
7.6.4 Checking Response Files 132
7.7 Using the Real-Time Monitor and Chart 132
7.7.1 Viewing the Real-Time Monitor 133
7.7.2 Viewing the Real-Time Chart 134
7.7.3 Changing the Real-Time Chart 135
7.8 Disconnecting Console Users 136
7.8.1 Disconnecting Users When Trevance® Runs As an Application 137
7.8.2 Disconnecting Users When Trevance® Runs As a Service 138

8 Maintenance 139
8.1 Maintenance Contract 139
8.2 Configure Warnings 140
8.3 Scheduling Database Maintenance 141
8.4 Backing Up and Restoring the Database Manually 143
8.5 Deleting Old Files 144
8.6 Sweeping the Database Manually 145
8.7 Verify/Repair 145
8.8 Archiving 146

9 PaymentVault™ 149
9.1 PaymentVault Server 149
9.2 UTID Storage 150
9.3 Configuring PaymentVault 151
9.4 Returning UTIDs from Trevance® 153
9.5 Batch Tokenize-Only 154
9.6 Real-Time Use of Tokenization 156
9.7 Real-Time UTID Updates 157

10 Reports and Emails 159

10.1 Configuring, Printing, and Saving Reports 159
10.1.1 Configuring Reports 159
10.1.2 Printing Reports 160
10.1.3 Saving Reports 161
10.2 Configuring and Sending E-Mail Notifications (Messages) 162

11 ACE: Auric Cipher Engine 169
11.1 Configuring Trevance® for ACE 169
11.2 Using Encrypted Account Values 170
11.3 ACE-Related Trevance® Error Messages 171
11.3.1 Online Encryption Failure 171
11.3.2 Online Decryption Failure 172
11.3.3 Batch Encryption Failure 172
11.3.4 Batch Decryption Failure 173

12 4250 Features 175
12.0.5 Real-Time Conditional Deposit Emulation 175
12.0.6 Settling Stored Transasctions 176
12.0.7 ValueLink and Disney Rewards Cards . . 178

13 Monitoring 179

14 Database Management 181
14.1 Restore 181
14.2 Recover 181
14.3 High Availability 182
14.3.1 Copying Recovery Logs on Windows . . . 182
14.4 Repair 183
14.5 Windows® 183

II External Key Management 185

15 akmp 187

III Payment Processors **189**

16 Chase Paymentech Solutions Direct/Salem **191**
16.0.1 Basic Settings . . . 192
16.0.2 Submitters . . . 193
16.0.3 Divisions . . . 194
16.0.4 Server . . . 196
16.0.5 Electronic Reports . . . 198
16.0.6 How Failover Works . . . 199
16.0.7 S-FTP Server with NetConnect . . . 200
16.0.8 How NetConnect Passwords Work . . . 202
16.0.9 Merchant Perspective . . . 203
16.0.10 Implementation Details . . . 203
16.0.11 NetConnect Batch Password Summary . 205
16.0.12 Configure Import Defaults for Batch Files 206
16.0.13 Configure Web Transaction Defaults . . . 208
16.0.14 Required Information . . . 213
16.0.15 Generally Useful Fields . . . 214
16.0.16 Advanced Configuration . . . 215
16.0.17 Important Refund Note . . . 236
16.0.18 PayPal . . . 236
16.0.19 PayPal Process Flow . . . 240
16.0.20 Revolution Money/Revolution Card . . . 244
16.1 Gift Cards . . . 249
16.1.1 Gift Card Specific Fields . . . 250
16.1.2 Gift Card Action Codes . . . 250
16.2 Account Updater . . . 256
16.2.1 Account Updater Action Codes . . . 257
16.3 Fraud Scoring . . . 257
16.3.1 Additional Fields . . . 258
16.3.2 Fraud Responses . . . 259
16.3.3 ValueLink . . . 263
16.4 Card-Type Indicator . . . 266

17 Chase Paymentech Solutions PNS/Tampa **269**
17.0.1 Server Info . . . 270
17.0.2 How Failover Works . . . 271
17.0.3 Divisions . . . 272

17.1 Configuring Transaction Defaults 274
17.1.1 Configure Web Transaction Defaults . . . 274
17.2 Methods of Payment, Actions, and Required Fields 276
17.2.1 Required Information 276
17.2.2 Supported Disney Rewards Cards Actions 277
17.2.3 Generally Useful Fields 279
17.2.4 Required PNS Configuration Settings . . 279
17.2.5 Timeouts and Duplicate Detection 280

18 First Data Compass Platform 281
18.1 Configuring Processor Settings 282
18.1.1 Basic Settings 282
18.1.2 Submitters 283
18.1.3 Divisions 284
18.1.4 Server 287
18.1.5 How Failover Works 289
18.2 Configuring Transaction Defaults 290
18.2.1 Configure Import Defaults for Batch Files 290
18.2.2 Configure Web Transaction Defaults . . . 292
18.3 Methods of Payment, Actions, and Required Fields 294
18.3.1 Important Information about Debit Cards 295
18.3.2 Required Information 296
18.3.3 Generally Useful Fields 298
18.3.4 Advanced Configuration 299
18.3.5 PayPal 309

19 Transfirst 319
19.1 Configuring Processor Settings 319
19.2 Methods of Payment, Actions, and Required Fields 323
19.2.1 Required Information 324
19.2.2 TransFirst-Specific Considerations 325
19.2.3 Generally Useful Fields 328
19.3 Advanced Transaction Configuration 329

20 Tsys 331
20.1 Configuring Processor Settings 331
20.2 Methods of Payment, Actions, and Required Fields 334
20.2.1 Required Information 335

20.2.2 Generally Useful Fields 340
20.3 Advanced Transaction Configuration 341
20.4 Generating an SSH Key 342
20.4.1 Generating 2048-bit RSA key with OpenSSH 342

IV PA DSS Secure Implementation Guide 345

1 Magnetic Stripe and CVV2 Data 347
1.1 General 347
1.2 Trevance® 348
1.2.1 Securely Delete Files 348
1.2.2 Proper Log Handling 349
1.2.3 Do Not Store CVV2 Field 349
1.3 CN!Express® 350
1.3.1 Securely Delete Files 350
1.3.2 Proper Log Handling 350
1.3.3 Do Not Store CVV2 Field 351
1.4 PaymentVault™ 351
1.4.1 Securely Delete Files 351
1.4.2 Proper Log Handling 351
1.4.3 Do Not Store CVV2 Field 351

2 Protect Stored Cardholder Data 353
2.1 General 353
2.2 Trevance® 354
2.2.1 Clearing Sensitive Data 355
2.2.2 Key Handling During Upgrade from Trevance® 2.x to Trevance® 3.x 356
2.3 CN!Express® 358
2.3.1 Clearing Sensitive Cardholder Data in Batch Transactions 359
2.3.2 Key Handling During Upgrade from CN!Express® 4.x to CN!Express® 5.x 360
2.4 PaymentVault™ 362
2.4.1 Re-Encrypting Historic Data 363

3 Secure Authentication Features 365

3.1 General . . . 365
3.2 Trevance® . . . 366
3.2.1 Replace Default Users . . . 366
3.3 CN!Express® . . . 367
3.3.1 Replace Default Users . . . 367
3.4 PaymentVault™ . . . 368

4 Log Payment Application Activity 369
4.1 General . . . 369
4.2 Trevance® . . . 370
4.3 CN!Express® . . . 372
4.4 PaymentVault™ . . . 374

5 Develop Secure Payment Applications 375
5.1 General . . . 375

6 Protect Wireless Transmissions 377
6.1 General . . . 377

7 Test Payment Applications to Address Vulnerabilities 379
7.1 General . . . 379

8 Facilitate Secure Network Implementation 381
8.1 General . . . 381

9 Cardholder Data Must Never Be Stored on a Server Connected To the Internet 383
9.1 General . . . 383

10 Facilitate Secure Remote Software Updates 385
10.1 General . . . 385

11 Secure Remote Access 387
11.1 General . . . 387
11.2 Trevance® . . . 388
11.3 CN!Express® . . . 388
11.4 PaymentVault™ . . . 389

12 Encrypt Sensitive Traffic **391**
12.1 General . . . 391
12.2 Trevance® . . . 391
12.3 CN!Express® . . . 391
12.4 PaymentVault™ . . . 392

13 Encrypt all Non-Console Administrative Access **393**
13.1 General . . . 393
13.2 Trevance® . . . 393
13.3 CN!Express® . . . 393
13.4 PaymentVault™ . . . 394

14 Maintain Instructional Documentation and Training Programs **395**
14.1 General . . . 395

V Appendices **397**

A Frequently Asked Questions **399**
A.1 Frequently Asked Questions . . . 399

B Troubleshooting Trevance® **405**

C Secure File Deletion **407**
C.1 General . . . 407
C.1.1 Quick Delete . . . 407
C.1.2 One-Pass Overwrite . . . 408
C.1.3 Multi-Pass Overwrite and Delete . . . 408
C.2 Trevance® . . . 408
C.3 CN!Express® . . . 409
C.4 PaymentVault™ . . . 409

D Error and Event Messages **411**
D.1 General Notes . . . 411
D.2 Trevance® Logs . . . 412
D.3 Configuration Report . . . 413
D.4 Events . . . 414
D.4.1 Server Management Events . . . 414

D.4.2 Error Reading or Writing Events 418
D.4.3 Real-Time Events 419
D.4.4 Batch Events 424
D.4.5 Method of Payment Events 428
D.4.6 Auric Cipher Engine™ (ACE) Events . . 429
D.4.7 PaymentVault™ Events 430

E Level III Transactions **433**
E.1 Purchase Card Line Items 433
E.2 Level III Line-Item Records 434
E.3 Importing 437
E.4 Exporting 439

F Contact Auric Systems International Technical Support **441**

List of Tables

1.1 Trevance® Versions and Abilities. 2

2.1 Installing Trevance 13

3.1 Configuring Imports 38
3.2 Change Default 41
3.3 Arrow Keys 45
3.4 Changing Field Position 46
3.5 Choices Under General 47
3.6 Moving Fields 58
3.7 Changing Field's Position 59
3.8 Moving from Boxes 63
3.9 Changing Fields Position 64
3.10 Preview 66
3.11 Importing/Exporting Configuration Information 76

4.1 Trevance® as a Service 86

5.1 Demo Test Production Mode Differences 95

6.1 Terms 108
6.2 Default File Extensions 111
6.3 Menus 115
6.4 Menus 117

7.1 Log Screen 124
7.2 Recent Batches Window 126
7.3 Submittal Queue 128
7.4 Real Time Monitor 134

8.1 Scheduling Database Maintenance 142

10.1 Email Notifications 164

16.1 Chase Paymentech Salem - Debit Card 212
16.2 Chase Paymentech Salem - Credit Card 216
16.4 Chase Paymentech Salem - Purchase Card (Level II) . 218
16.5 Chase Paymentech Salem - Purchase Card (Level III) . 219
16.6 Chase Paymentech Salem - Third-Party Encrypted Card 220

16.7 Chase Paymentech Salem - Electronic Checks 221
16.8 Chase Paymentech Salem - Third-Party Encrypted Electronic Checks 222
16.9 Chase Paymentech Salem - Switch/Solo 223
16.10Chase Paymentech Salem - PIN-less Debit 223
16.11Chase Paymentech Salem - PIN-based Debit 225
16.12Chase Paymentech Salem - PIN-based Debit 2 226
16.13Chase Paymentech Salem - (ARC) 227
16.14Chase Paymentech Salem - POP 229
16.15Chase Paymentech Salem - Bill Me Later 230
16.19Chase Paymentech Salem - PayPal 237
16.20Chase Paymentech Salem - Retail Credit Card Swipe . 242
16.21Chase Paymentech Salem - Retail Credit Card Manually Entered 243
16.22Chase Paymentech Salem - Card Not Present 245
16.23Chase Paymentech Salem - Card Present Transactions 247
16.24Gift Card Actions 250
16.25Account Updater Action Codes 257
16.26Optional Fields for Safetech Fraud 258
16.27Safetech Fraud Response Fields 259
16.28Chase Paymentech Salem - ValueLink Fields 263

17.1 Chase Paymentech PNS - Disney Rewards Card Actions 278

18.1 First Data Compass - Debit Card Info 295
18.2 First Data Compass Credit Card 299
18.4 First Data Compass - Purchase Card (Level ll) 301
18.5 First Data Compass - Purchase Card (Level lll) 302
18.6 First Data Compass - Electronic Checks 304
18.7 First Data Compass - PIN-less Debit 304
18.8 First Data Compass - Bill Me Later 306
18.9 First Data Compass - European Direct Debit 308
18.10First Data Compass - Pay Pal 310
18.11First Data Compass - Retail Credit Card Swipe 316
18.12First Data Compass - Retail Credit Card: Manually Entered 317

19.1 Trans First - Credit Card 325

19.2 Trans First - Purchase Card (Level ll) 326
19.3 Trans First - Electronic Checks 327

20.1 Tsys - Credit Card 337
20.2 Tsys - Purchase Card (Level ll) 337
20.3 Tsys - Accounts Receivable Check Conversion (ARC) . 339

A.1 ASI Response Codes 400

E.1 Level III Specific Fields 433
E.2 Line Item Samples 435
E.3 Importing 437

List of Figures

8.1 Network Installation 381

1 Welcome

Thank you for selecting the Trevance® payment processing application. Trevance® provides high-speed real-time authorization of transactions with high-volume batch processing. It is your direct connection to your processing service.

Trevance® offers the following features (depending on the capabilities of your processing service):

- Simultaneously processes both real-time and batch transactions
- Processes real-time authorizations at 30 transactions per second (sustained)
- Handles batches easily exceeding 200,000 transactions
- Supports many methods of payment including:
  - Credit card (MasterCard, Visa, American Express, Discover, etc.)
  - Purchase card (levels 2 and 3)
  - Electronic checks
  - ARC (accounts receivable check conversion)
  - POP (point of purchase check conversion)
  - PIN-based debit card
  - PINless debit card
  - European Debit
  - Bill Me Later®
  - PayPal™
  - Retail (card swipe) as well as Card Not Present
- Uses Federally-approved 256-bit AES encryption for sensitive data
- Offers built-in web interface for real-time authorizations
- Is PCI validated.
- Table 1. 1 shows the capabilities of the different Trevance® versions.

Table 1.1: Trevance® Versions and Abilities.

Model #	*Capabilities*	*Processing Service*
CN-3500	Batch only ARC Credit Cards Electronic Checks PayPal Purchase Cards	Chase Paymentech Solutions First Data First National Merchant Services (FNMS)
CN-4200	High speed and batch 50 real-time transactions per second Bill Me Later European debit [1] Google Checkout [1] Green Dot Money Pak™ [1] PayPal PIN-based debit [1] PINless debit [1] POP Revolution Card [1] Value Link Card [1]	Chase Paymentech Solutions First Data

Continued on next page

Table 1.1 – *Continued from previous page*

Model #	*Capabilities*	*Processing Service*
CN-4250	High speed and batch 50 real-time transactions per second Additional Functionality Auto Settlement Bill Me Later European debit [1] Google Checkout [1] Green Dot Money Pak™ [1] PayPal PIN-based debit [1] PINless debit [1] POP Revolution Card [1] Value Link Card [1]	Chase Paymentech Solutions First Data

[1] Chase Paymentech Methods of Payment Functionality

1.1 PCI Compliance

PCI in regards to software refers to the Payment Card Industry compliance rules; especially the Payment Application Data Security Standard (PA-DSS) standards. Trevance® undergoes a third-party validation to ensure it meets the PCI PA-DSS requirements. This ensures the software is suitable for your use within a PCI-compliant environment. Additionally, Auric Systems International is now a validated Level 1 PCI Service Provider.

1.2 Passwords

Trevance® uses passwords at several different levels:

- Access to the underlying operating system.
- Encrypting sensitive data.
- Submitting transactions through the Web.
- Monitoring Trevance®.

Your in-house PCI policy in regards to password and key management must be applied to these passwords.

1.3 Access to the Underlying Operating System

All Trevance® configuration is performed locally. There is no remote access for configuration and control.

1.4 Encrypting Sensitive Data

Trevance® supports an external key management server accessible via the Auric Key Management Proxy (AKMP). Please refer to Chapter 15, for security-specific information.

1.5 Submitting Transactions through the Web

Trevance® requires all web-based transactions to include a user ID and password. These accounts cannot retrieve any information from Trevance® beyond the information returned for the current transaction. Trevance® limits the IP addresses from which web transactions are accepted.

1.6 Contacting Auric Systems International

To contact Auric Systems International:

Phone	603-924-6079
E-mail/support	support@AuricSystems.com
E-mail/sales	sales@AuricSystems.com
Web Site	http://www.AuricSystems.com

You can also reach the Auric Systems International home page directly from the Trevance® Help menu:

- Click on Help.
- Click on Auric Systems International Home Page.

When you call or e-mail, please have your serial number handy. When you purchased Trevance®, the serial number and activation key were e-mailed to you. After you install the test or production (live) Trevance®, you can find your serial number and activation key on the Run Mode Tab of the Trevance® Settings Manager.

Part I

Installation and Configuration

2 Installing Trevance®

This chapter describes the minimum and recommended system requirements for Trevance®, and how to install and uninstall the software on your computer system. It also explains how to change the ADMIN password.

Trevance® always installs in demonstration (demo) mode. In demo mode, you can switch among the different versions that support your processing service (for example from a CN-3500 demo to a CN-4200 demo).

2.1 Minimum and Recommended System Requirements

2.1.1 Minimum System Requirements

Trevance® **requires**:

- A minimum of 512 Mbytes of memory
- A 1 Gigahertz Pentium Processor (CN-3500)
- A 2.5 Gigahertz Pentium Processor (CN-4200)
- A TCP/IP network connection for the computer where Trevance® is installed

Trevance® runs on any of the following platforms:

- Windows XP
- Windows 7
- Windows Server 2008 R2

For initial installation, you'll need approximately 100 Mbytes of hard disk space.

2.1.2 Recommended System Requirements

You should test Trevance® in demo mode on your target platform to see how it performs. To get the best performance from CN-3500, use Windows Server 2008 on a machine with 2 GHz processor or better and with a minimum of 1 Gbyte of memory.

CN-4200, running at peak load, performs best on a dual-core 2 GHz processor with 2 Gbyte of memory. You should keep a minimum of 30 Gbytes of free disk space to ensure a long-lived and trouble-free installation.

Additional information about system requirements is available at www.AuricSystems.com.

2.1.3 Important Information

Your processing service has its own minimum operating requirements. Contact your processing service directly for more information.

2.2 Installing Trevance®

2.2.1 Installation Options

Trevance® is always installed on your system:

- As both an application and a Windows service (the Windows service is not active)
- In the demonstration (demo) mode (not in the test or production mode)
- As a CN-3500 demo

After installation you can change any of those defaults.

When you're configuring Trevance®, Auric Systems International strongly recommends that you:

- Run Trevance® as an application (not a service).
- Configure using the demo mode.
- Send your first transaction(s) to your processing service using the test mode.

Demo mode is ideal for trying out configuration options and Trevance® operations without affecting real transactions. Test mode is ideal for testing your configuration with your processing

service. Production mode is strictly for processing real transactions.

Once you've configured and tested Trevance®, you can switch to the production mode and you can run Trevance® as a service (see page 125), confident that Trevance® will work smoothly.

2.2.2 Installation Procedure

1. Begin the installation from the Auric Systems International web page: www.AuricSystems.com. Go to Downloads and follow the instructions for downloading Trevance® payment software.

2. The following screen appears:

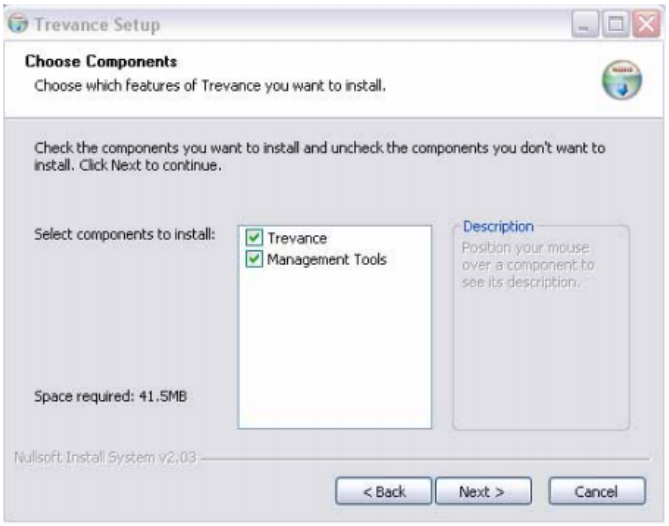
Trevance Setup
Welcome to the Trevance Setup Wizard
This wizard will guide you through the installation of Trevance.
It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.
Click Next to continue.
Next >
Cancel

3. Click on to view:

Trevance Setup
License Agreement
Please review the license terms before installing Trevance.
Press Page Down to see the rest of the agreement.
LICENSE AGREEMENT
TERMS AND CONDITIONS
PLEASE CAREFULLY READ ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT PRIOR TO CONTINUING USE OF THIS PROGRAM. CONTINUING USE OF THIS PROGRAM CONSTITUTES YOUR ACCEPTANCE OF THESE TERMS AND CONDITIONS. IF YOU DO NOT AGREE WITH THE FOLLOWING TERMS AND CONDITIONS, NO LICENSE IS GRANTED HEREUNDER, AND YOU ARE NOT AUTHORIZED TO USE THIS PROGRAM.
1. LICENSE: You have the non-exclusive right to use the following Trevance(tm)
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Trevance.
Nullsoft Install System v2.03
< Back
I Agree
Cancel

4. Read the license screen. Print it if you like. Click on

to accept the license and to view a screen like the following:


Trevance Setup
Choose Components
Choose which features of Trevance you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.
Select components to install:
Trevance
Management Tools
Description
Position your mouse over a component to see its description.
Space required: 41.5MB
Nullsoft Install System v2.03
< Back
Next >
Cancel

5. Do one of the following:

Table 2.1: Installing Trevance

Install	*Procedure*	*Notes*
TREVANCE AND MANAGEMENT TOOLS	Check-mark at both items (default)	Recommended
TREVANCE ALONE*	Remove check-mark next to Management Tools	*Not recommended*
MANAGEMENT TOOLS ALONE*	Remove check-mark next to Trevance Transaction Gateway	Used for monitoring Trevance from a remote system

*If you install just the management tools, you can install Trevance® later by repeating this installation procedure from Step 1. At Step 5, remove the check-mark from Management Tools but leave the check-mark at Trevance® Transaction Gateway.

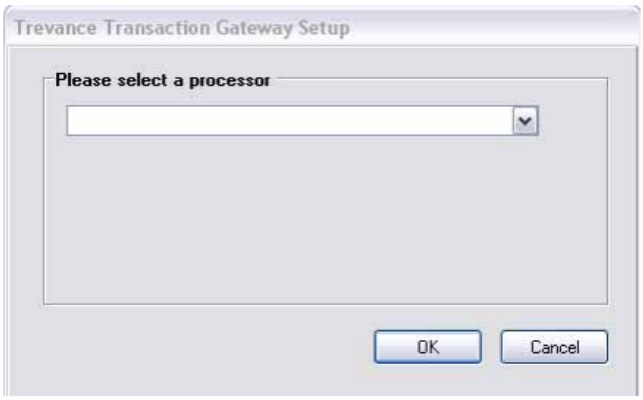
6. Click on Next > to view a screen like the following:

Trevance Setup
Choose Install Location
Choose the folder in which to install Trevance.
Setup will install Trevance in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.
Destination Folder
C:\Program Files\Trevance
Browse...
Space required: 41.5MB
Space available: 56.2GB
Nullsoft Install System v2.03
< Back
Install
Cancel

The Space Required and Space Available figures let you know if you have enough space on your computer to install Trevance®. If you don't, cancel the installation until you have created enough space.

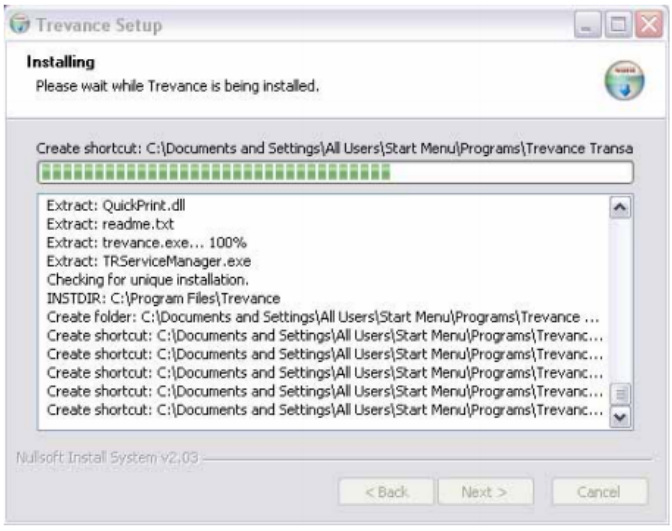
To change the default installation directory, click on Browse...

7. Click on Install to view:

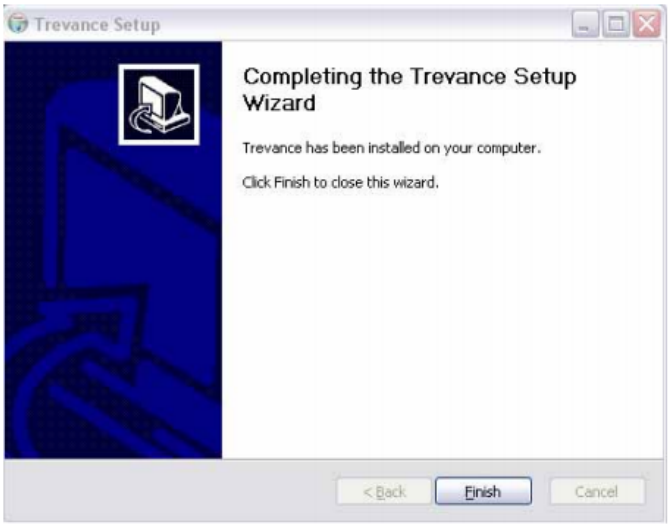


8. Select your processing service.

9. Click on OK to view a screen like the following:


Trevance Setup
Installing
Please wait while Trevance is being installed.
Create shortcut: C:\Documents and Settings\All Users\Start Menu\Programs\Trevance Transa
Extract: QuickPrint.dll
Extract: readme.txt
Extract: trevance.exe... 100%
Extract: TRServiceManager.exe
Checking for unique installation.
INSTDIR: C:\Program Files\Trevance
Create folder: C:\Documents and Settings\All Users\Start Menu\Programs\Trevance ...
Create shortcut: C:\Documents and Settings\All Users\Start Menu\Programs\Trevanc...
Create shortcut: C:\Documents and Settings\All Users\Start Menu\Programs\Trevanc...
Create shortcut: C:\Documents and Settings\All Users\Start Menu\Programs\Trevanc...
Create shortcut: C:\Documents and Settings\All Users\Start Menu\Programs\Trevanc...
Create shortcut: C:\Documents and Settings\All Users\Start Menu\Programs\Trevanc...
Nullsoft Install System v2.03
< Back
Next >
Cancel

10. Wait. The following screen appears:



11. Click on Finish

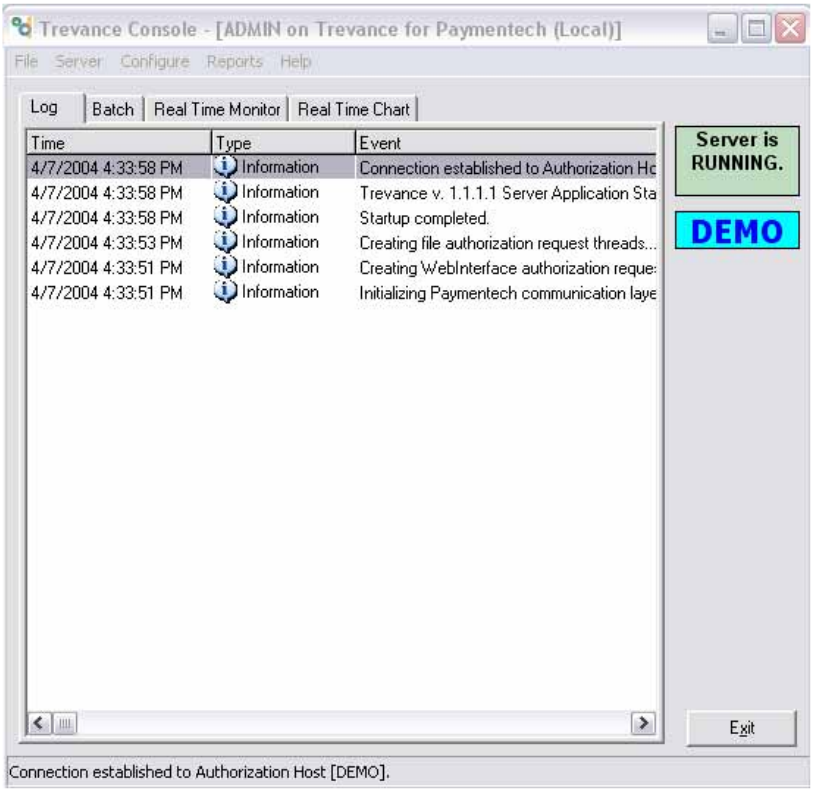
    Trevance® is now installed

2.3 Starting Trevance® the First Time

1. Click on start
2. Click on All Programs
3. Click on Trevance® Transaction Gateway.
4. Click on Trevance® to view a screen like the following:

5. In the Password box, type **ADMIN.**

6. A screen like the following appears:


Trevance Console - [ADMIN on Trevance for Paymentech (Local)]
File Server Configure Reports Help
Log
Batch
Real Time Monitor
Real Time Chart
Time
Type
Event
4/7/2004 4:33:58 PM Information Connection established to Authorization Hc
4/7/2004 4:33:58 PM Information Trevance v. 1.1.1.1 Server Application Sta
4/7/2004 4:33:58 PM Information Startup completed.
4/7/2004 4:33:53 PM Information Creating file authorization request threads...
4/7/2004 4:33:51 PM Information Creating WebInterface authorization reque:
4/7/2004 4:33:51 PM Information Initializing Paymentech communication laye
Server is RUNNING.
DEMO
Exit
Connection established to Authorization Host [DEMO].

This main Trevance® screen may differ slightly depending on your processing service. Trevance® is in demo mode

7. Click on Configure.

8. Click on *Pause Server to Configure Items Below*. You are prompted to confirm.

   Trevance® is now ready for configuration.

Trevance® installs with a default ADMIN user (default password ADMIN) that allows you to change processor settings and directories, for example. To protect your system, before you change anything else, delete the default ADMIN user and create a new administrator as described on page 22.

2.4 Creating a New Administrator (and Web User)

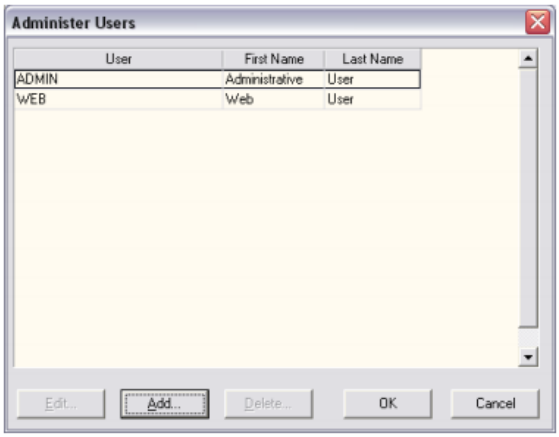
Trevance® installs with a default ADMIN user (and a default WEB user) to get you started. You can work with Trevance® using these defaults. But before you test Trevance® and before you can send real transactions to your processing service, you must replace and delete the default ADMIN user. If you're using a web interface, you must also replace and delete the default WEB user. These changes are necessary for PCI compliance.

PCI standards say that you can't use any default accounts shipped with a product. To help you comply, Trevance® refuses to run in test or production (live) mode if an account exists with the user name ADMIN. If you're using the web interface, Trevance® refuses to run in test or production mode if an account exists with the user name WEB. As a result, you must create at least one new user with administrative privileges (an administrator) and then delete the default ADMIN user. Now is a good time to do that. You'll be all set for the switch from demo to test to production mode.

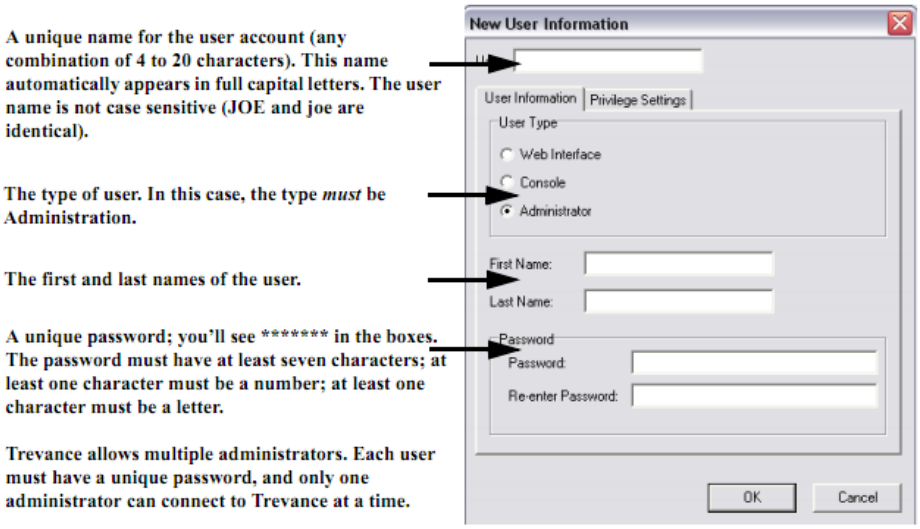
An administrator is able to make changes and take special actions that are barred to web and console users. Only an administrator can delete the default ADMIN user. That's why Trevance® refuses to allow you to delete the default ADMIN user until you've created a new administrator.

2.4.1 Creating a New Administrator

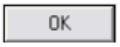
1. Click on Configure.
2. Click on Users to view:



3. Click on to view:


A unique name for the user account (any combination of 4 to 20 characters). This name automatically appears in full capital letters. The user name is not case sensitive (JOE and joe are identical).
The type of user. In this case, the type must be Administration.
The first and last names of the user.
A unique password; you'll see ******* in the boxes. The password must have at least seven characters; at least one character must be a number; at least one character must be a letter.
Trevance allows multiple administrators. Each user must have a unique password, and only one administrator can connect to Trevance at a time.
New User Information
User Information
Privilege Settings
User Type
Web Interface
Console
Administrator
First Name:
Last Name:
Password
Password:
Re-enter Password:
OK
Cancel

4. Fill in the boxes under the USER INFORMATION tab.
   You *must* choose Administrator.
5. You don't have to click on the PRIVILEGE SETTINGS tab; it simply confirms that administrators have no privilege restrictions.

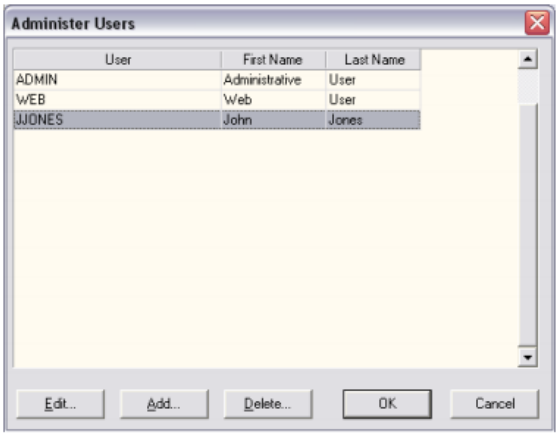
6. Click on 

7. Exit Trevance®.

The first time you log in as the new administrator, you must type the user name and password exactly as they appear in the NEW USER INFORMATIONscreen. Thereafter, the user name appears automatically.

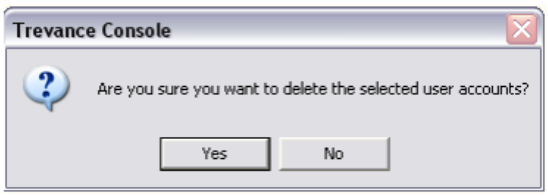
2.4.2 Deleting the Default ADMIN User

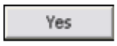
1. Make sure you've logged into Trevance® using the new administrator name and password you just created. Do not log in as the default ADMIN user.
2. Click on Configure.
3. Click on Users to view:



4. Click on the ADMIN user name.
5. Click on

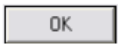
   Trevance® displays the following message:



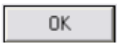
6. Click on 

   Trevance® displays a message like the following:

7. Click on

8. Click on 

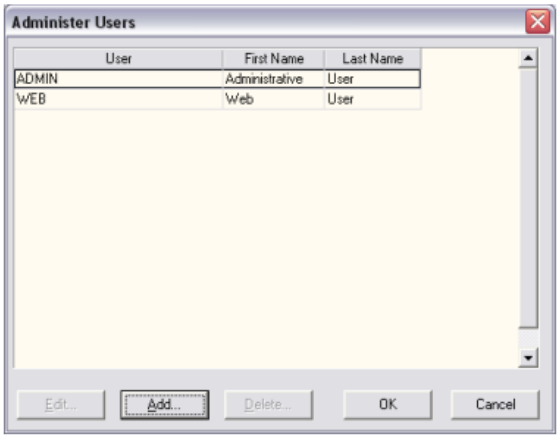
again, to exit the ADMINISTER USERS screen.

9. Click on 

10. From now on, when you log in as an administrator, you must use the new password. *You can't log in without your password.*

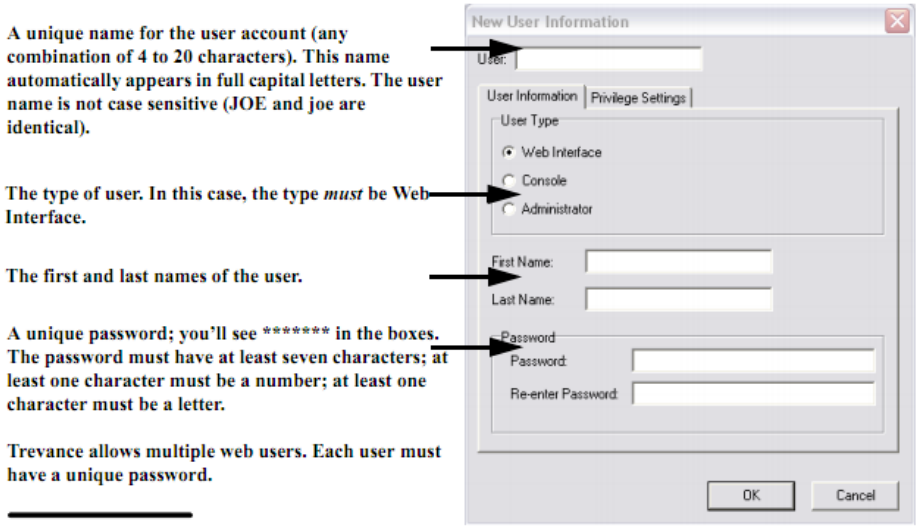
2.4.3 Creating a New Web User

1. Click on Configure.
2. Click on Users to view:



3. Click on

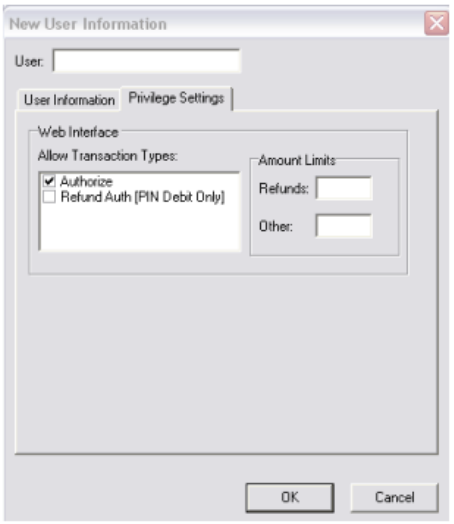
to view:


A unique name for the user account (any combination of 4 to 20 characters). This name automatically appears in full capital letters. The user name is not case sensitive (JOE and joe are identical).
The type of user. In this case, the type *must* be Web Interface.
The first and last names of the user.
A unique password; you'll see ******* in the boxes. The password must have at least seven characters; at least one character must be a number; at least one character must be a letter.
Trevance allows multiple web users. Each user must have a unique password.
New User Information
User:
User Information
Privilege Settings
User Type
Web Interface
Console
Administrator
First Name:
Last Name:
Password
Password:
Re-enter Password:
OK
Cancel

4. Fill in the boxes under the USER INFORMATION tab.

   You *must* choose Web Interface.

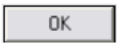
5. Click on the PRIVILEGE SETTINGS tab to view:



6. Select the Transaction Types: Authorize only, Refund Auth only, or both.

7. Type in the Amount Limits to set the highest amount that is allowed for a single refund and/or other transaction at this

web site. If the box is left blank, the web site can transfer any amount. The default is any amount.

8. Click on 

2.4.4 Deleting the Default WEB User

Take the same steps you used to delete the default ADMIN user (see page 24).

3 Configuring Trevance®

This chapter describes the general Trevance® configuration.

The main tasks in setting up Trevance® are:

- Configure password
  Change your current password.
- Configure users
  Add and delete users and change the user information.
- Configure reports
- Configure e-mail notification
  Arrange to receive hourly, batch, daily, and other notifications by e-mail.
- Configure Warnings
- Turn off certain import warnings.
- Configure scheduled database maintenance
- Configure processor settings
  Enter the information Trevance® needs to communicate with your specific processing service; this information is provided by the processing service.
- Configure the web interface
  Tell Trevance® what to expect from the web interface and what information to send back. Turn web processing on or off.
- Configure imports for batch files
  Tell Trevance® what type of information it should expect from your external application and in what format.
- Configure exports for batch files
  Tell Trevance® what type of information it should send to the external application and in what format.
- Configure the AKMP key management proxy
- Configure directories
  Change the default directories where files are stored.
- Configure options

- Decide whether to start in paused mode, how long to track duplicate orders, whether to change the default file extensions, and whether to use file polling, among other options.
- Configure serial number and activation key, and set the mode (demo, test, or production)
- Produce a configuration report
  The configuration report shows exactly the configuration you've set up and also lets you transport your configuration information (except for passwords) from one installation to another.
- Set run mode
- Run demo as
  Switch between CN-3500 and CN-4200 for Chase Paymentech Solutions while in demo mode.

3.1 Preparing for Configuration

3.1.1 Using the Demonstration Version and Running Trevance® As an Application

When you're configuring Trevance® for the first time, it is best to work in the demo mode and run Trevance® as an application. Trevance® automatically installs in demo mode and as an application (it also installs as a Windows® service, but the service is not active).

After you complete the configuration, you can test it without sending transactions to your processing service. When you're satisfied with the configuration, you can switch from demo to test mode and then to production mode. You can also switch to running Trevance® as a service. Trevance® automatically remembers the configuration you set up when it was in demo mode and running as a application. Trevance® uses that same configuration when you switch modes and/or run it as a service.

You may work in demo mode using the default ADMIN user and (if you are using a WEB interface) the default WEB user. But Trevance® won't let you test your configuration or really process

transactions until you've deleted the default ADMIN user and created one or more new administrators. You should have made this change already, but if you haven't, now is a good time.

3.1.2 Running the Trevance® Console and Server on the Same Machines

For security, Configuration must occur on the same machine that is running the Trevance® payment application. Note that the Trevance® Console by default now writes all output data to the user's documentation directory under the Trevcon subdirectory. For example, if the user name under which you run Trevance® is auricuser, the Trevance® Console writes logs and exports into C:\Documents and Settings\auricuser\Trevcon. This behavior has been changed in order to support Windows 7 and Server 2008.

3.1.3 Pausing Trevance®

To configure imports and exports, you must pause Trevance® first. If Trevance® is running, the choices on the Configure menu are disabled (you can't select them). Make sure Trevance® is paused. If necessary, do one of the following:

- Click on Configure, then click on *Pause Server to Configure Items Below*
- Click on Server, then click on Pause.

3.1.4 Checking the File Extension

Trevance® requires every file to have a specific extension. For import files, the default extension is .IMP (you can change this).

Trevance® will process any file as long as the file name ends with the correct file extension. Suppose Trevance® is set up to use the default file extension (.IMP) for imports. In that case:

- The following file names are all acceptable for import files: ABC.IMP or ABC.FFF.IMP or ABC_FFF.IMP. (The file names are not case sensitive: for example, abc.imp and abc_FFF.imp are also acceptable.)

- The following file names are *not* acceptable: ABC.FFF or ABC.IMP.FFF or ABC_FFF. Trevance® ignores import files with an incorrect extension.

If your computer hides extensions, you can't check the file names. With "hide extensions" in effect, a file that is named ABC.IMP.FFF is listed on screen as ABC.IMP. The file name looks right, but Trevance® ignores the file because its real (hidden) extension is .FFF, not .IMP.

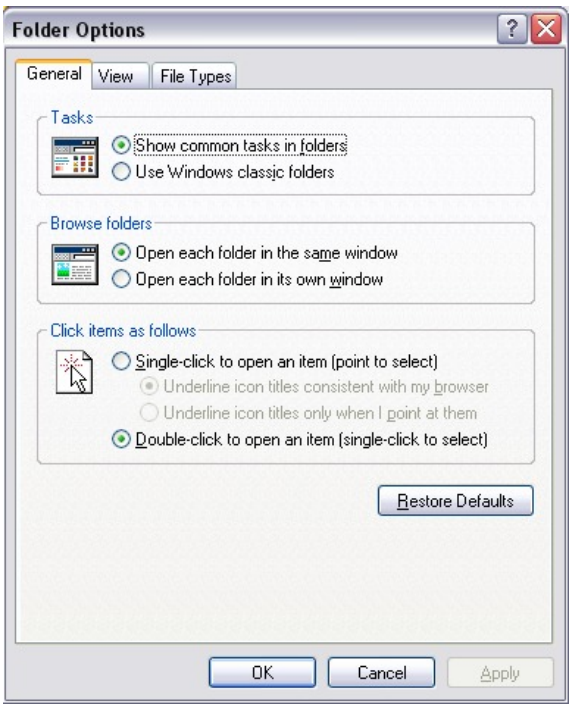
To show and check the extensions on your files:

1. Right click on

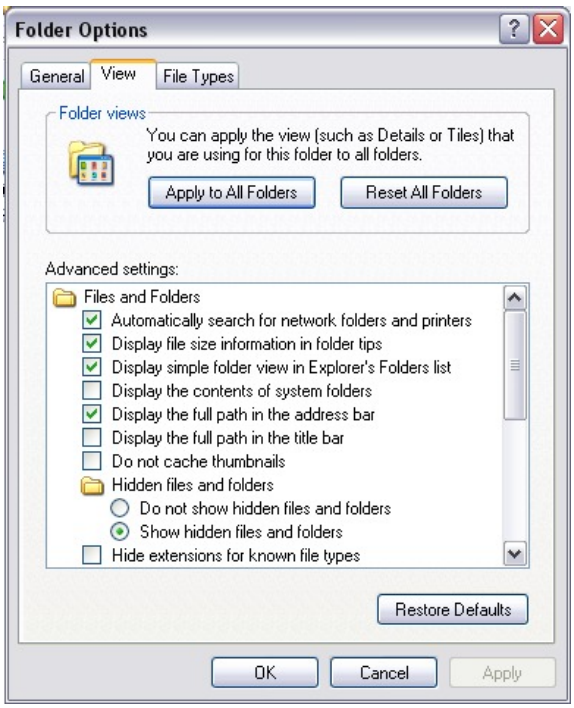
2. Click on Explore.

3. Click on the C: drive.

4. On the Tools menu, click on Folder Options to view a screen like the following:



5. Click on the View tab to view:

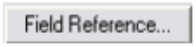

Folder Options
General
View
File Types
Folder views
You can apply the view (such as Details or Tiles) that you are using for this folder to all folders.
Apply to All Folders
Reset All Folders
Advanced settings:
Files and Folders
Automatically search for network folders and printers
Display file size information in folder tips
Display simple folder view in Explorer's Folders list
Display the contents of system folders
Display the full path in the address bar
Display the full path in the title bar
Do not cache thumbnails
Hidden files and folders
Do not show hidden files and folders
Show hidden files and folders
Hide extensions for known file types
Restore Defaults
OK
Cancel
Apply

6. Make sure the Hide file extensions box is unchecked; if there's a check-mark, click on the box to remove the check-mark.
7. Click on OK
8. Using Windows Explorer, check the file extensions on your files in Trevance®'s BATCHIMPORT directory.
9. If necessary, rename the files so they only have one extension.

3.1.5 Understanding Fields

Trevance® imports and exports fields, such as account number or order date, containing information about each transaction. For more information about the fields available with your processing service:

1. Click on Help.
2. Click on Field Reference.

You may also access the field reference list during import and export configuration. Click on 

3.1.6 Restarting the Console When It Times Out

During configuration (or whenever an administrator is signed on), the Trevance® console times out after 15 minutes of inactivity. This measure helps keep Trevance® secure even if the administrator leaves Trevance® open and running.

If you need to restart the Trevance® console:

1. Double click the icon on the task bar of your desktop:
2. Click on

3. Log in.

3.1.7 Saving Configuration Information

At any time, you can request a configuration report that shows exactly the configuration you've set up. If you then copy this report to a word processing program (for example), you can save it for future reference. If you change that configuration and decide later on to re-create it, the information you need is in the report.

To create the report:

1. Click on Help.
2. Click on Configuration Report.
3. Click on

The screen closes.
4. Immediately open a new document in a text editor or word processing program.
5. Paste.
6. Save the pasted configuration report.

More information about the configuration report appears later in this chapter.

3.1.8 Configuring Currencies

The examples in this manual use U.S. dollars. Trevance® currently supports over 150 world currencies. Specific currency support is dependent on your processor.

Currencies are selected when configuring merchant ids (divisions).

Some processing services do not allow multiple currencies.

3.2 Adding, Deleting, and Administering Users

You can add and delete users, and change their user information.

The three types of users are administrator, web, and console. Each type of user has different privileges; the administrator has all privileges. You may create more than one user of each type. Multiple web and console users may log in at the same time, but only one administrator may log in at a time.

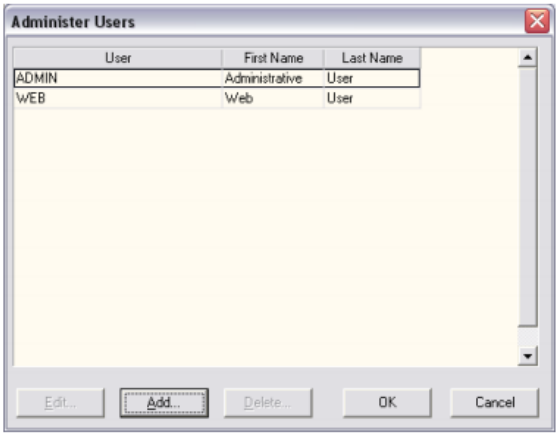
You may work in demo mode using the default ADMIN user and (if you are using a web interface) the default WEB user. But Trevance® won't let you test your configuration or really process transactions until you've created a new administrator and deleted the default ADMIN user. You should have made this change already, but if you haven't, now is a good time.

3.2.1 Adding a User

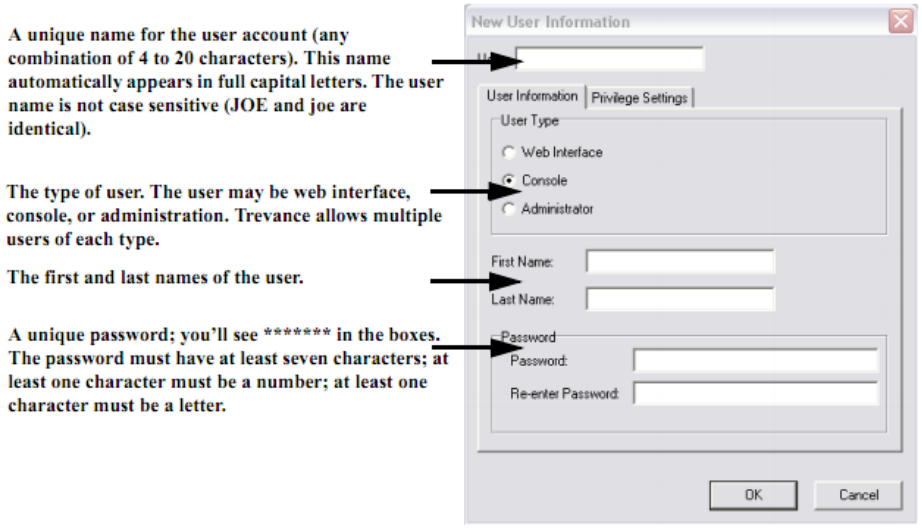
You might want to add separate users to the system to handle batch files, archives, and other tasks. If you are using Trevance® to process transactions from several web sites, you might want to add a separate "web user" for each web site so that you can track transactions separately.

To add a user to the system:

1. Make sure you are logged into the system as an administrator.
2. Click on Configure.
3. Click on Users to view:



4. Click on to view:

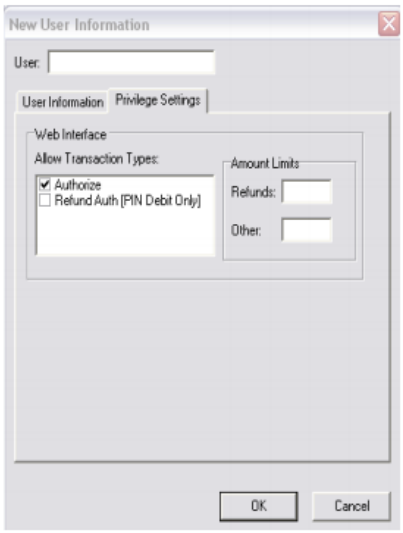

A unique name for the user account (any combination of 4 to 20 characters). This name automatically appears in full capital letters. The user name is not case sensitive (JOE and joe are identical).
The type of user. The user may be web interface, console, or administration. Trevance allows multiple users of each type.
The first and last names of the user.
A unique password; you'll see ******* in the boxes. The password must have at least seven characters; at least one character must be a number; at least one character must be a letter.
New User Information
User Information
Privilege Settings
User Type
Web Interface
Console
Administrator
First Name:
Last Name:
Password
Password:
Re-enter Password:
OK
Cancel

5. Fill in the boxes under the User Information tab.

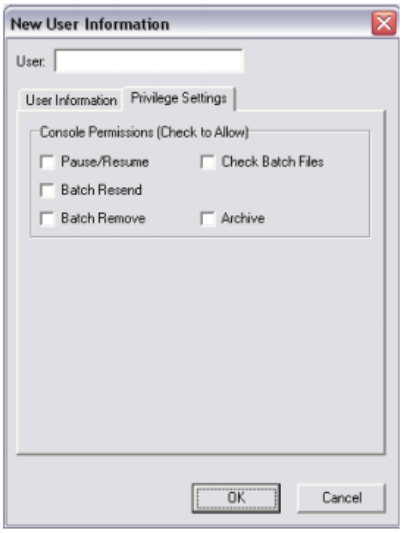
   You may choose Web Interface *or* Console *or* Administration as the User Type. The default User Type is Console.

6. Click on the Privilege Settings tab. The screen that appears depends on the User Type you selected. For an administrator, the screen simply confirms that no privilege restrictions exist. The screens for Web Interface and Console users are:

If you selected Web Interface as the User Type, the following Privilege Settings are available:



If you selected Console as the User Type, the following Privilege Settings are available:



7. Under Privilege Settings for a web user:
   - Select the Transaction Types: Authorize only, Refund Auth only, or both.
   - Type the Amount Limits under Web Interface to set the highest amount that is allowed for a single transaction at this web site. If the box is left blank, the web site can transfer any amount. The default is any amount.

   Under Privilege Settings for a console user:
   - Click on any or all of the boxes to add a check-mark if you want the user to perform that task (for example, a check-mark next to archive means that this particular user can archive). The default is no check-mark.

8. Click on OK

9. Click on OK

The first time a new user logs in, the user must type his or her user name and password as they appear in the New User Information screen. The name must be spelled correctly, but Trevance® is case insensitive. Thereafter, the user name appears automatically.

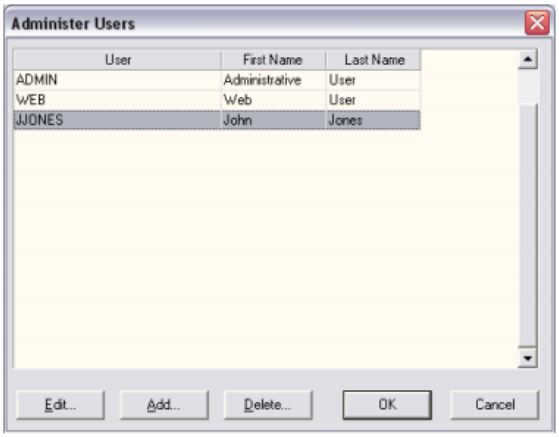
If the user forgets the password, an administrator is the only person who can change it.

3.2.2 Changing User Information

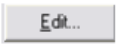
1. Click on Configure.

2. If the server isn't paused, click on *Pause Server to Configure Items Below*.

3. Click on Users to view:



4. Click on the user's name (in this example, JJONES).

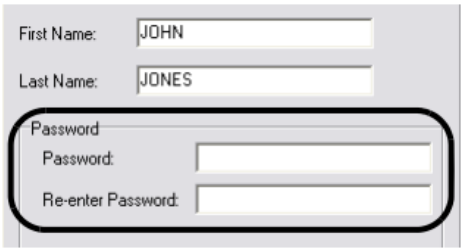
5. Click on  to view:

6. Change any information you want to change under the User Information and Privilege Settings tabs.

7. To change the password, click on to view a screen like the following:

8. Type your administrator password in the Password box. (The password appears as a series of asterisks: *******.)

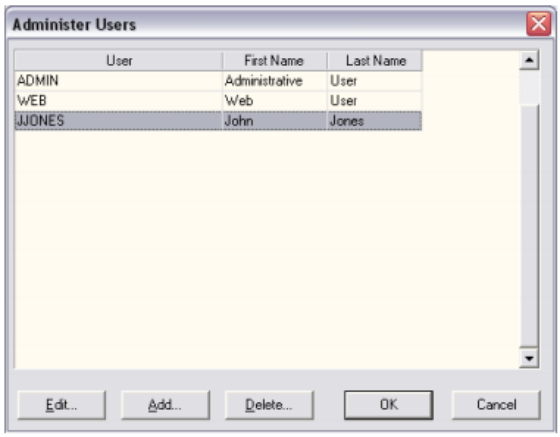
9. Click on to view:



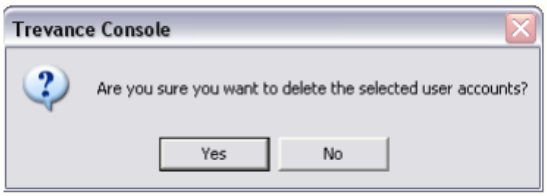
10. Type the new password into the unlocked Password box. (The password appears as a series of asterisks: *******.)
11. Type the password again in the Re-enter Password box. (The password appears as a series of asterisks: ********.)
12. Click on OK to enter the changes you've made.
13. Click on OK to save your changes and exit the Administer Users screen.

3.2.3 Deleting a User

1. Click on Configure.
2. If the server isn't paused, click on *Pause Server to Configure Items Below*.
3. Click on Users to view:



4. Click on the user's name (in this case JJONES).
5. Click on Delete to remove the user from the user list. Trevance® displays the following message:



6. Click on Yes

   Trevance® displays a message like the following:

7. Click on OK

8. Click on OK again, to save your changes and exit the Administer Users screen.

3.3 Configuring Processor Settings

Trevance® needs information about your processing service to communicate with your processing service's computer. Most of this information varies for each processing service. Before changing any processor settings, read the relevant chapter in "Part II. Your Processing Service" (starting on page 193), and check with your processing service.

3.3.1 Configuring Imports for Batch Files

External applications send and receive delimited text files. They send files to Trevance® for processing by the processing service, and then receive the results back as delimited text files.

Using the Configure Import screen, you tell Trevance® what to expect: the contents and organization of each file. Purchase Card Level III has a hard-coded format to which import fields need to conform. So there are no import (or export) configuration options for Purchase Card Level III (see "Appendix B. Level III Transactions" on page 353).

After configuration, Trevance® expects every import file to contain the information you've specified in the order you specified. Trevance® automatically reformats the transactions in the file to meet the requirements of your processing service.

The following procedure makes two assumptions:

- The imported text file uses a tab for the delimiter and has quotation marks around fields.

- You're using a file supplied with Trevance® to configure imports.Trevance® comes with sample, processor-specific files for use during formatting. (You could use any file of your own with the extension .IMP, .TXT, or .CSV.)

The sample file you use for configuration must reside on the same machine you're configuring from; you can configure imports from a remote computer, but the sample file must be located on the remote computer.

The sample file supplied in the BATCHIMPORT directory contains a small number of credit card transactions.

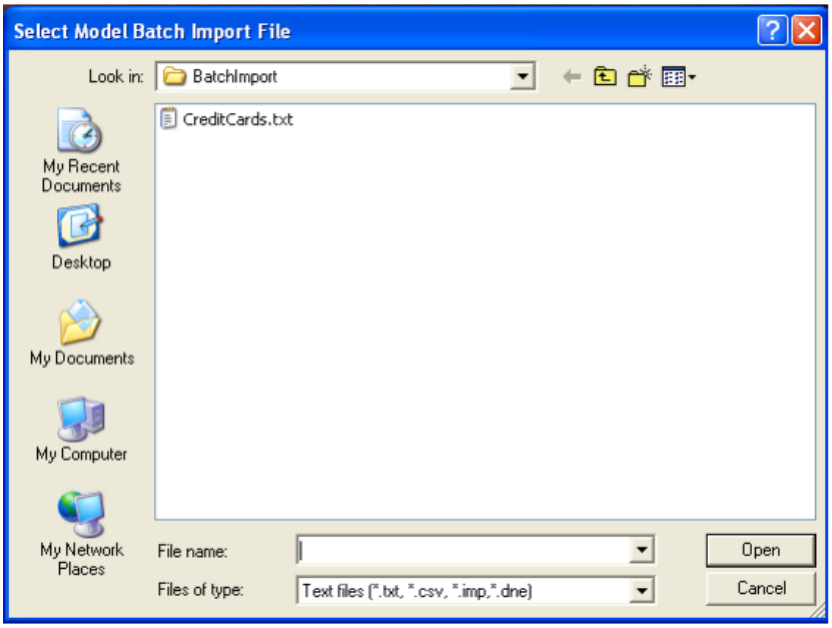
To configure imports for batch files:

1. Click on Configure.

2. If the server isn't paused, click on *Pause Server to Configure Items Below*.

3. Click on Batch Files.

4. Click on Imports to view:



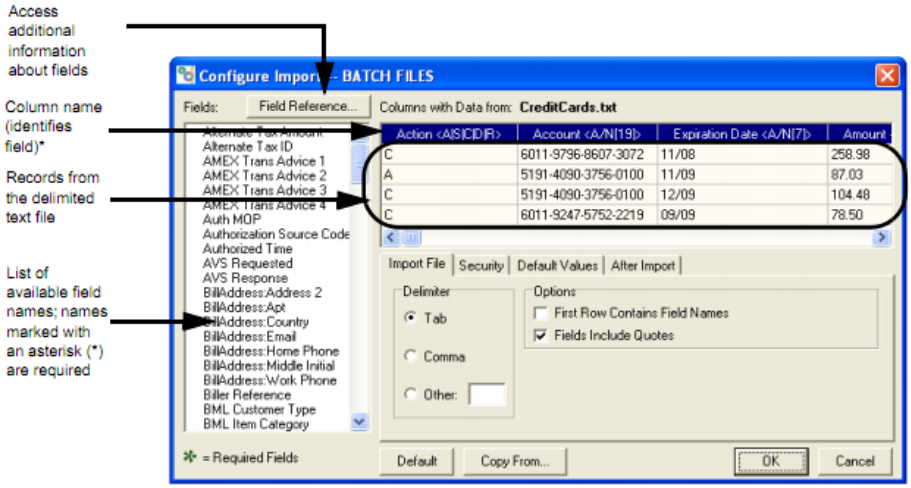
5. Double click on the text file containing the types of transactions you will be doing:

Table 3.1: Configuring Imports

Name of File	*Processing Service*
CreditCards.txt	Just Credit Cards

You can configure imports using any file with a .TXT, or .CSV, or .IMP extension; but for actual processing, Trevance® only accepts files with a .IMP extension.

In the following procedure, the CreditCards.txt file is used. The file you choose to work with appears on a screen like the following:



*The column name contains information about the field. For example, <A/N[19]> indicates an alphanumeric field that has a maximum size of 19 characters.

Each record is a transaction. The records in your text file appear nicely separated on the screen, with the fields in individual columns.

6. Make sure that every column has the correct field name assigned to it. For example, the column called Account must actually show account numbers.

   If a column is marked Unassigned and you don't assign a field name to it, that column of information isn't sent to your processing service. Unassigned columns aren't imported.

   To change column names, you have three choices: use the default button, copy a previous configuration, or select fields one-by-one.

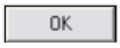
   - Click on Default

     Trevance® provides the default fields and arranges them in a default order. You can click on the default button at any time.

   - Click on Copy From... to view a screen like the following:

Select Copy Source
This will copy the settings (fields, field sequence, etc.) from one type of import/export specification to another.
Copy Settings From
Batch Export
OK
Cancel

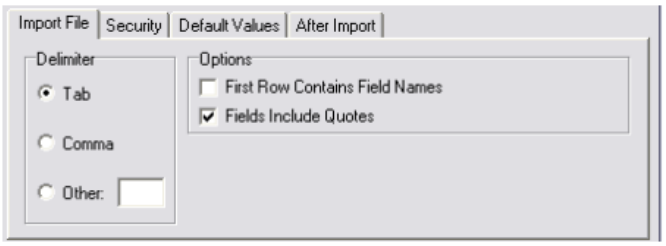
This screen lets you copy a configuration that you've created previously for batch export.

Click on 

Trevance® copies the column names and their order from the export configuration.

- Click on a field name in the Fields list, then drag the name to the head of the column.
  If you place your selection over an existing column name (for example, replacing BillAddress with ShipAddress), the old name automatically returns to the Fields list.

7. Click on the Import File tab to view:

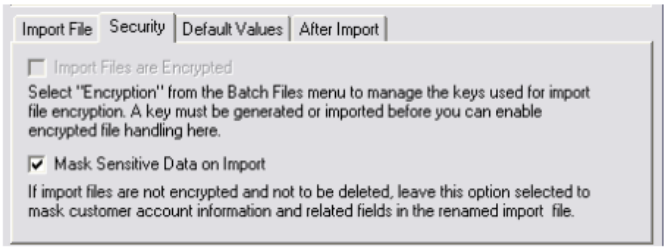


8. Click on a radio button to identify the Delimiter used by the imported text file. The default delimiter is a tab.
9. If necessary, click on one of the choices under Options to change the default:

Table 3.2: Change Default

Option	*No Check-Mark*	*Check-Mark*
First Row Contains Field Names	Assumes that the first row of text is the record of a transaction, not a list of field names (default).	Assumes that the first row of text contains field names.
Fields Include Quotes	Assumes that any quotes are part of the transaction record and includes them in the record sent to the processing service (default).	Assumes that any quotes around a field aren't part of the transaction and deletes the quotes.

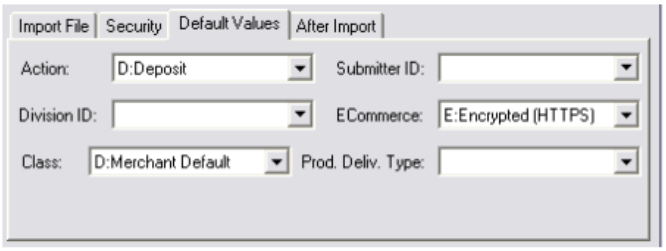
10. Click on the Security tab to view:


Import File
Security
Default Values
After Import
Import Files are Encrypted
Select "Encryption" from the Batch Files menu to manage the keys used for import file encryption. A key must be generated or imported before you can enable encrypted file handling here.
Mask Sensitive Data on Import
If import files are not encrypted and not to be deleted, leave this option selected to mask customer account information and related fields in the renamed import file.

11. The method for generating an encryption key is described on page 75. After you've generated the encryption key, you can return to this tab. If you decide to encrypt import files, place a check-mark next to Encrypt Import Files. For now, go on to Step 12.

12. By default, a check-mark appears next to Mask Sensitive Data on Import. Masking hides part of the customer account information in renamed import files (for example, in .DNE files). It has no effect on the screen or on export files. Masking obscures all but the last four characters of a credit card number and entirely obscures the CVV (so that number 1000-0001-0001 appears as ****-****-0001). If you remove the check-mark, sensitive data is not masked in the file.

13. Click on the Default Values tab to view:

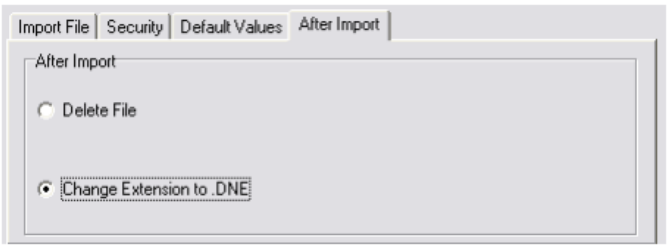


14. If your import file doesn't specify an Action field for each transaction, you must set the default Action to one of the choices (such as Authorize or Deposit). For example, if you select Authorize, every transaction that Trevance® receives with a blank Action field is assumed to be an authorization.

15. You may need to change other defaults, such as Division ID, Class (merchant default, MOTO, recurring, or E-commerce), Tender (credit card, purchase card, or check), Submitter ID, Prod.

Type (for example, gift certificate or shareware), and ECommerce (for example, non-secure or secure). The choices that appear depend upon (a) your processing service and (b) the information you entered when configuring processor settings (such as submitter and division ID information).

16. Click on After Import to view:



Here you tell Trevance® how to handle the import file after importing it. The default to change the extension of the real-time or batch file from .IMP to .DNE, and then save it. The file is renamed (or deleted, if you change the default) as soon as it is successfully loaded into the Trevance® database.

17. When your configuration is finished, click on OK to leave the Configure Import screen.

3.4 Configuring Exports for Batch Files

After your processing service approves or declines the transaction, it sends the result back to Trevance® . Trevance® prepares the processed transaction for export to your external application.

With the Configure Exported Files screen, you tell Trevance® what type of information (which fields) to export to your external application and in what format. If you don't select a field, the information isn't saved in the export file, even if your processing service included it. For an explanation of all the fields available for export, see the Field Reference under the main Help menu.

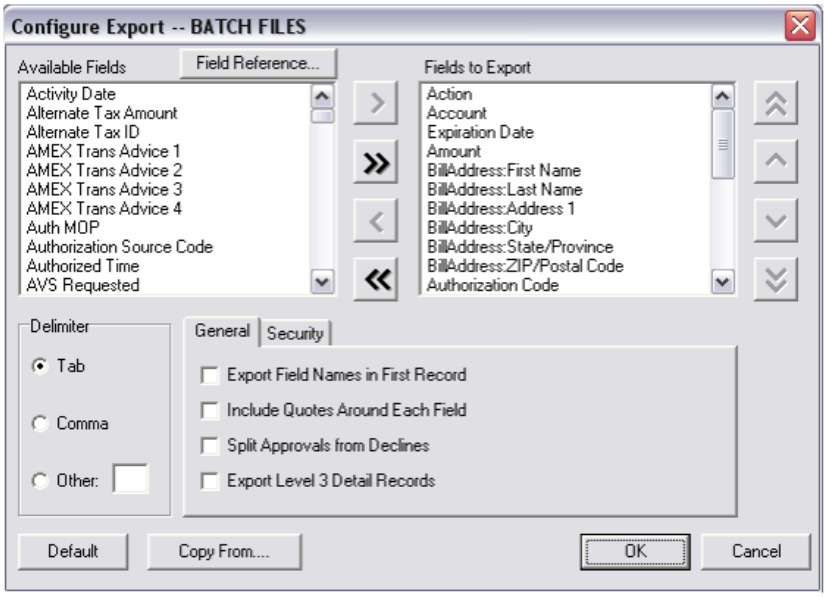
Purchase Card Level III has a hard-coded format to which import fields need to conform. So there are no export (or import)

configuration options for Purchase Card Level Level III (see "Appendix B. Level III Transactions" on page 353).

The sample file you use for configuration must reside on the some machine you're configuring from; you can configure exports from a remote computer, but the sample file must be located on the remote computer.

To configure exports for batch files:

1. Click on Configure.
2. If the server isn't paused, click on *Pause Server to Configure Items Below*.
3. Click on Batch Files.
4. Click on Exports to view a screen like the following:



5. There are two main boxes on the Configure Export screen: Available Fields and Fields to Export. Initially, Fields to Export displays the default set of export fields. You may want to export additional fields. For example, if you add the Response Text field, you'll be able to see why the processing service declined a transaction. That information may tell you how to fix your import configuration to reduce the number of declines.

For information about individual fields, click on Field Reference...

6. To move a field from one box to the other, select the field by clicking on the field name. Then either drag and drop the fields to the list or use the arrow keys.
   - Suppose you drag Activity Date to the Fields to Export list. It will be placed above the item you drag it to. The fields in the Fields to Export box should be listed in order of appearance in the record for each transaction.
   - If you decide to drag Activity Date back to the Available Fields list, it will automatically be placed in alphabetical order, regardless of where you drop it.
   - To use the arrow keys:

Table 3.3: Arrow Keys

Click on...	*To...*
	Move the selected field into the FIELDS TO EXPORT box
	Move all the available fields into the FIELDS TO EXPORT box
	Move the selected field into the AVAILABLE FIELDS box (that field REDO THIS exported)
	Move all the fields into the AVAILABLE FIELDS box (no fields are exported)

7. The first field shown in the Fields to Export box is the first field to appear in the record for each transaction. To change

a field's position, select the field by clicking on the field name. Then:

Table 3.4: Changing Field Position

Click on...	*To Move a Field . . .*
	To the top spot in the box (the beginning of the record)
	Up one spot
	Down one spot
	To the bottom spot in the box (the end of the record)

Trevance® arranges each transaction record to show the fields you chose at Step 3, in the order you chose at Step 4.

To return all fields to their default position (with the original fields listed in their original order in the Fields to Export box), click on

8. If necessary, change the defaults under Delimiter and General:

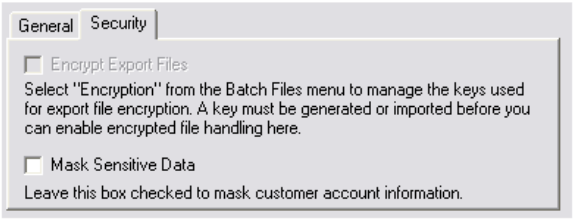
Step 9 and Step 10 describe the choices offered in each box.

9. Click on a radio button to choose a Delimiter. The default delimiter is a tab.
10. Click on any of the choices under General:

Table 3.5: Choices Under General

Option	*No Check-Mark*	*Check-Mark*
Export Field Names in First Record	Doesn't show the field names for the fields you selected at Step 3 (default)	Shows the field names for the fields you selected at Step 3
Include Quotes Around Each Field	Omits quotes around field names (default)	Places quotes around fields
Split Approvals from Declines	Places all transactions (approved and declined) in a single .EXP file in the BATCHEXPORT directory (default)	Places approved transactions in a .OK file in the BATCHEXPORT directory, and declined transactions in a .BAD file in the DECLINES directory

11. Click on the Security tab to view:


General
Security
Encrypt Export Files
Select "Encryption" from the Batch Files menu to manage the keys used for export file encryption. A key must be generated or imported before you can enable encrypted file handling here.
Mask Sensitive Data
Leave this box checked to mask customer account information.

12. The method for generating an encryption key is described in page 75. After you've generated the encryption key, you can return to this tab. If you decide to encrypt export files, place a check-mark next to Encrypt Export Files. For now, go on to Step 13.

13. By default, a check-mark does *not* appear next to Mask Sensitive Data.

    If you place a check-mark next to Mask Sensitive Data, part of the customer account information is hidden in export files (for example, in OK files). It has no effect on the screen or on import files. Masking obscures all but the last four characters of a credit card number (so that 1000-0001-0001 appears as 0001).

14. When you've configured your export files the way you want them,

    click on

3.5 Generate Server Passphrase and Batch File Encryption Key

Trevance® uses a passphrase as an encryption key to protect your data. This security feature is not optional.

In addition, you may encrypt batch export files by generating an encryption key for use by your external encryption/decryption program. This security feature is optional.

You must first generate the server passphrase. Then you can generate or import an encryption key for use by your external encryption or decryption program. You may also export the key.

3.5.1 Generate Server Passphrase

Before switching to either test or production mode, you must enter a passphrase for your server. Trevance® uses the passphrase as an encryption key to protect your data. To simplify initial configuration and testing, Trevance® uses a default encryption key in demo mode.

For added security, the passphrase is broken into two segments. Each segment may be known by only one person, so that two people are required to enter the entire passphrase. Each segment of the passphrase:

- Is case sensitive (for example, ABC4567ghi1234 is different from ABC4567GHI1234, where ABC4567 is the first segment).

- Must contain both letters and numbers (punctuation marks are also allowed).

- Must be at least seven characters long.

Create and archive the two passphrase segments according to your corporate policy. Additional information on passphrase maintenance is available in the document *Payment Application Best Practices for Trevance®* .

The server passphrase is stored in the current user's account. You *must* set the passphrase while the Trevance® server is logged in as the same user that will run Trevance®— in test or production mode.

1. Click on Configure.

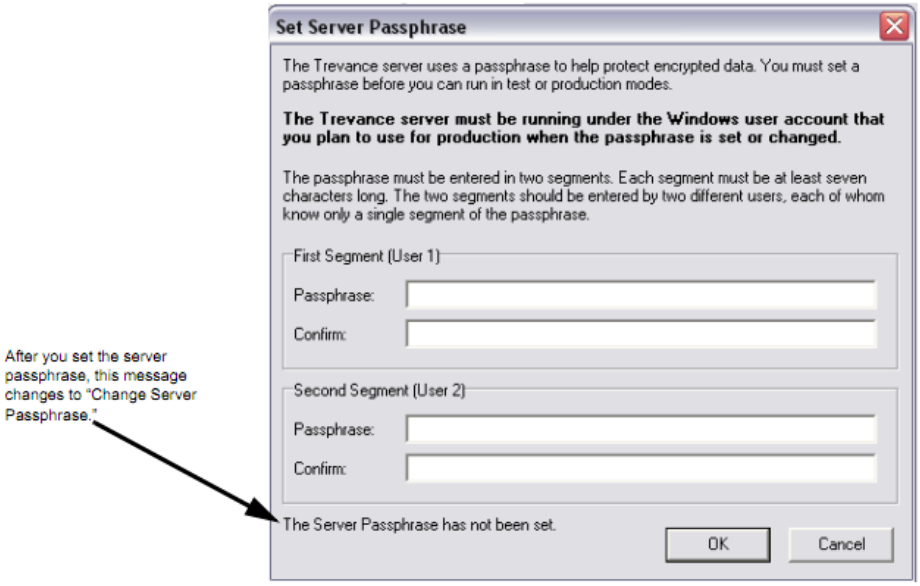
2. If the server isn't paused, click on *Pause Server to Configure Items Below*.

3. Click on Batch Files.

4. Click on Encryption to view:

Trevance Console
You must set the server passphrase before you can modify Batch Encryption settings.
Do you want to set the server passphrase now?
Yes
No

5. Click on to view:


Set Server Passphrase
The Trevance server uses a passphrase to help protect encrypted data. You must set a passphrase before you can run in test or production modes.
The Trevance server must be running under the Windows user account that you plan to use for production when the passphrase is set or changed.
The passphrase must be entered in two segments. Each segment must be at least seven characters long. The two segments should be entered by two different users, each of whom know only a single segment of the passphrase.
First Segment (User 1)
Passphrase:
Confirm:
Second Segment (User 2)
Passphrase:
Confirm:
The Server Passphrase has not been set.
OK
Cancel
After you set the server passphrase, this message changes to "Change Server Passphrase."

6. Type each segment into the given Passphrase box, then retype it at confirm.

7. Click on OK to view:

8. Click on OK

9. You are now ready to generate or import an encryption key.

3.5.2 Generate, Import, or Export an Encryption Key

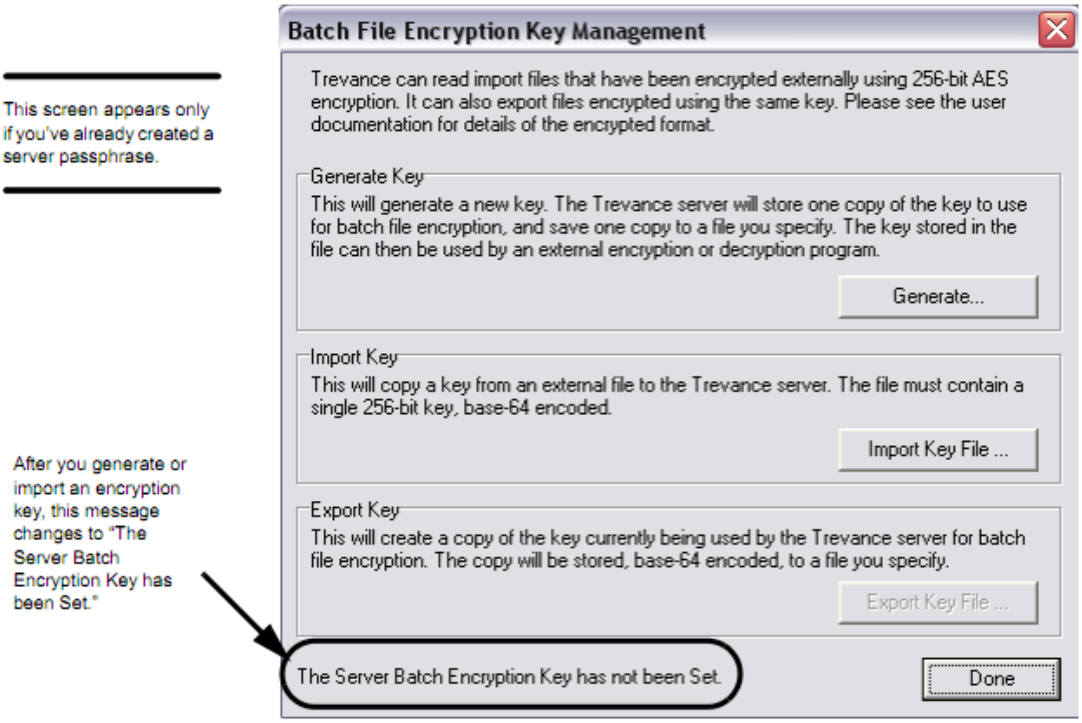
After you generate or import an encryption key, you may configure batch file imports and/or exports for encryption, as described earlier.

1. Click on Configure.

2. If the server isn't paused, click on *Pause Server to Configure Items Below*.

3. Click on Batch Files to view this message:

4. Click on Encryption to view a screen like the following:


This screen appears only if you've already created a server passphrase.
After you generate or import an encryption key, this message changes to "The Server Batch Encryption Key has been Set."
Batch File Encryption Key Management
Trevance can read import files that have been encrypted externally using 256-bit AES encryption. It can also export files encrypted using the same key. Please see the user documentation for details of the encrypted format.
Generate Key
This will generate a new key. The Trevance server will store one copy of the key to use for batch file encryption, and save one copy to a file you specify. The key stored in the file can then be used by an external encryption or decryption program.
Generate...
Import Key
This will copy a key from an external file to the Trevance server. The file must contain a single 256-bit key, base-64 encoded.
Import Key File ...
Export Key
This will create a copy of the key currently being used by the Trevance server for batch file encryption. The copy will be stored, base-64 encoded, to a file you specify.
Export Key File ...
The Server Batch Encryption Key has not been Set.
Done

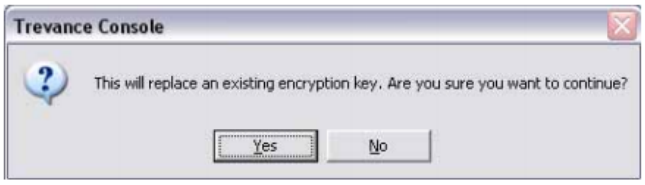
5. To automatically generate a new encryption key, go to Step 6.

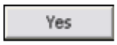
   To import the key, go to Step 11.

   To export the key, go to Step 17.

Generating a New Encryption Key

6. Click on to view:



7. Click on 

The encryption key is generated and stored in the database. You then have the option of saving the key to an external file. A screen like the following appears:

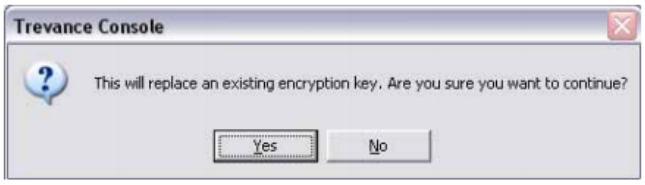
8. Browse to the location where you want to save the encryption key.
9. Click on

10. Click on

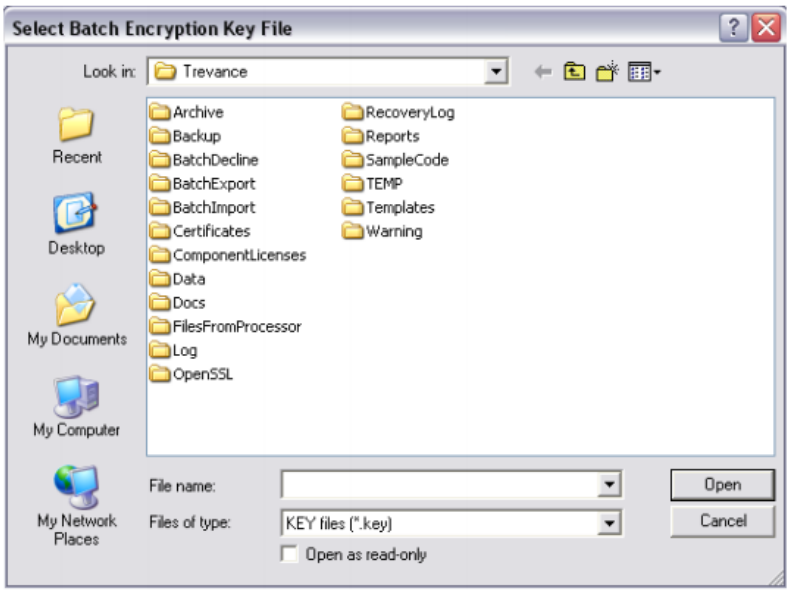
Importing Encryption Key

11. To import a new encryption key, click on

to view:



12. Click on Yes to view a screen like the following:



13. Type in the File name.
14. Browse to the location where you want to save the encryption key.
15. Click on Open
16. Click on OK

Exporting Encryption Key

17. To export an encryption key, click on Export Key File ... to view a screen like the following:

18. Browse to the location where you want to save the encryption key.
19. Click on Save
20. Click on OK
21. When you've finished managing the encryption key, click on Done

3.6 Configuring the Real-Time Web Interface

Trevance® accepts authorization transactions or authorization refunds (for debit cards) from any application capable of sending and receiving an HTTP POST; for example, an interactive voice response (IVR) system, a relational database, or a program written in any of the dozens of computer languages that can communicate using web standards. Each web request (POST) contains one transaction. Trevance® handles up to 15 POSTs per second.

Use the Web Interface Settings screen to see the fields your application should be sending to the web (the (Web Request Format) and

to configure the response Trevance® receives (the Web Response Format).

Using the Web Request Format screen, you indicate the delimiter, any URL encoding, and other characteristics of the POST that Trevance® will receive. Then, Trevance® automatically arranges the transaction from your application to meet the requirements of your processing service. The Web Request Format screen is a guide.

Using the Web Response Format screen, you tell Trevance® what to send back to the web application, after your processing service has accepted or declined the transaction. You select the fields and the order in which you want them to appear, among other options. With the Web Response Format screen, you actually configure the response Trevance® sends.

The following sections give separate instructions for configuring each form on the Web Interface Settings screen. You can also move from tab to tab (from form to form) and then save all your changes at once, without leaving the screen.

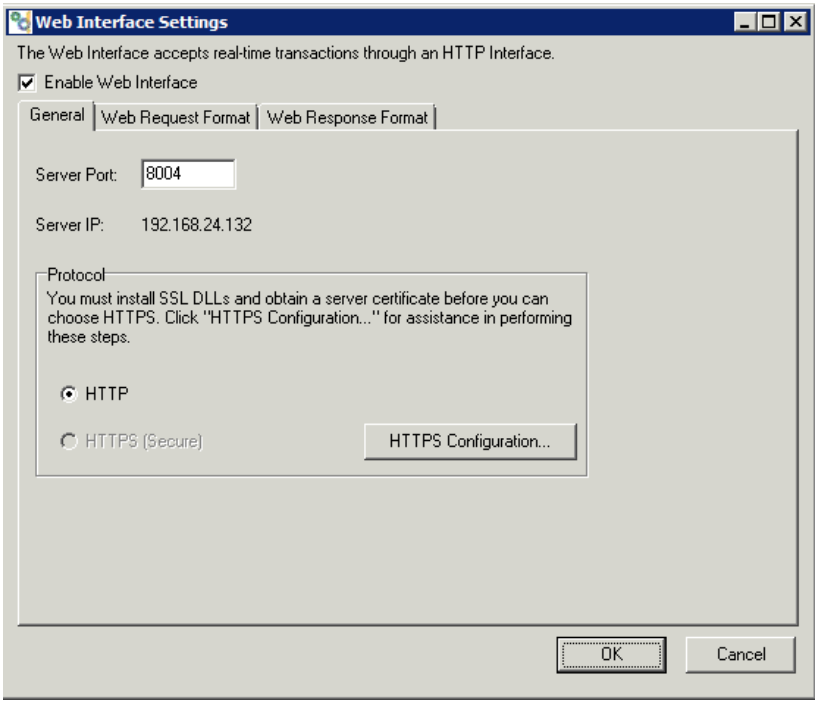
Look in Trevance® s SampleCode directory for examples of how to talk to the web server using various programming languages.

3.6.1 Enable Web Interface and Change Server Port

1. Click on Configure.

2. If the server isn't paused, click on *Pause Server to Configure Items Below*.

3. Click on Real Time Web Interface to view:



4. To enable the web interface, you must have a check-mark in the Enable Web Interface box. The default is no check-mark (web interface is *not* enabled). Click on the box to add the check-mark.
5. Click on the General tab.
6. If necessary, change the server port number.
7. To use HTTPS, rather than HTTP you must first install SSL DLLs and obtain a server certificate. For further information, click on the HTTPS Configuration box
8. Click on OK

3.6.2 Formatting the Web Request

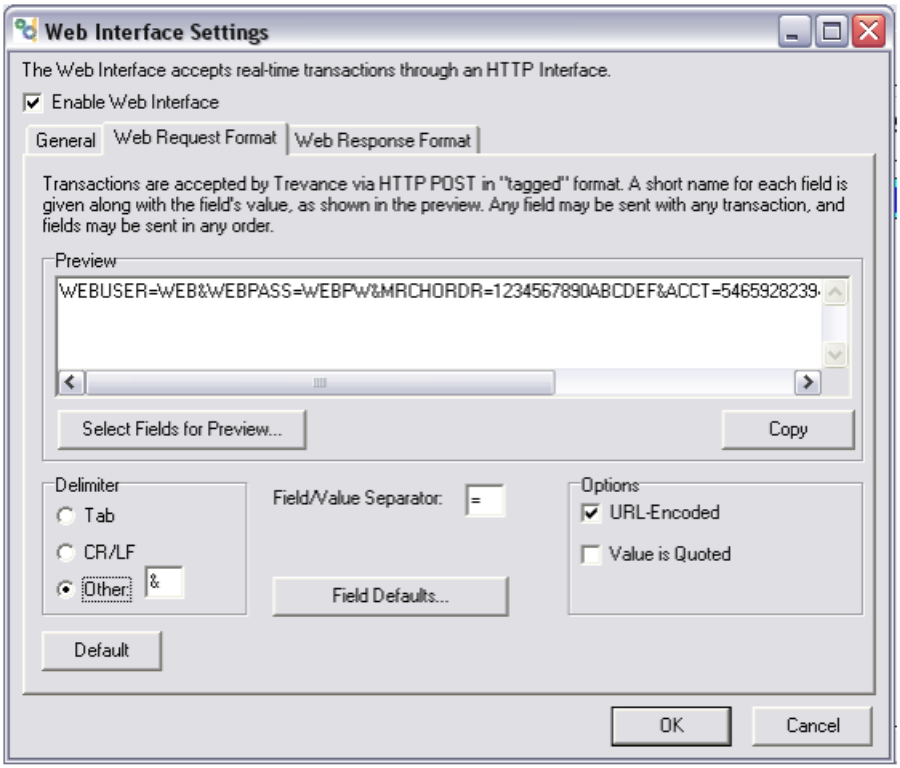
Transactions are sent to the Trevance® web interface in a simple tagged format. You don't have to configure this format, since any field can be sent in any order in the request. However, you must specify:

- The character you intend to use as a delimiter (the default is an ampersand, &)
- The character you intend to use as a field value separator (the default is an equal sign, =)

The Web Request Format screen lets you specify those characters and also build sample text strings showing a selection of fields formatted with those characters.

The text string (shown in the Preview) is a guide and example only; you can send any valid fields your process requires, as long as they are properly formatted with the correct delimiters. The fields don't have to show up in the Preview.

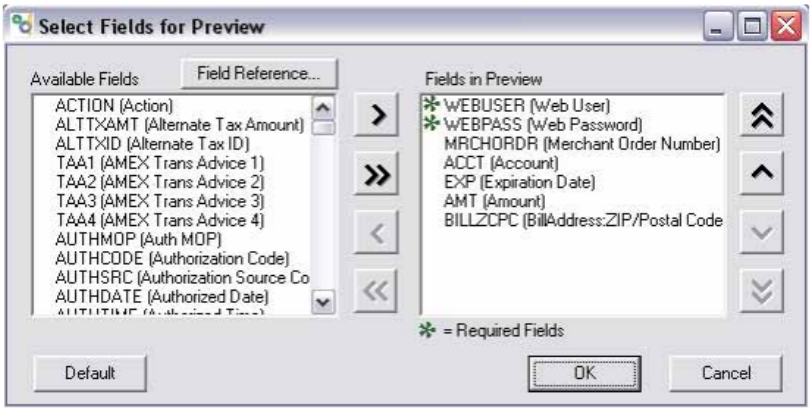
1. Click on Configure.
2. If the server isn't paused, click on *Pause Server to Configure Items Below*.
3. Click on Real Time Web Interface, then the Web Request Format tab to view:



The Preview box shows the effects of changes you make. At any time, you can return to the original defaults (including those in the Preview box) by clicking on the Default button.

4. Click on

to view:



5. There are two main boxes on the Select Fields for Preview screen: Available Fields and Fields in Preview. Some of the default fields are shown in the screen above. You may want to change or add to these fields.

   To move a field from one box to the other, select the field by clicking on the field name. Then:

Table 3.6: Moving Fields

Click on...	*To . . .*
	Move the selected field into the Fields in Preview box)
	Move all the available fields into the Fields in Preview box

Continued on next page

Table 3.6 – *Continued from previous page*

Click on...	*To...*
	Move the selected field into the Available Fields box (that field isn't exported)
	Move all the fields into the Available Fields box (no fields are exported)

6. The first field shown in the Fields in Preview box is the first field to appear in the Preview. To change a field's position, select the field by clicking on the field name. Then:

Table 3.7: Changing Field's Position

Click on...	*To Move a Field . . .*
	To the top spot in the box (the beginning of the record)
	Up one spot
	Down one spot

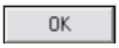
Continued on next page

Table 3.7 – *Continued from previous page*

Click on...	*To Move a Field . . .*
	To the bottom spot in the box (the end of the record)

Trevance® arranges each transaction record to show the fields you chose at Step 3, in the order you chose at Step 4.

7. To return all fields to their default position (with the default fields listed in their original order in the Fields in Preview box), click on

8. Click on 

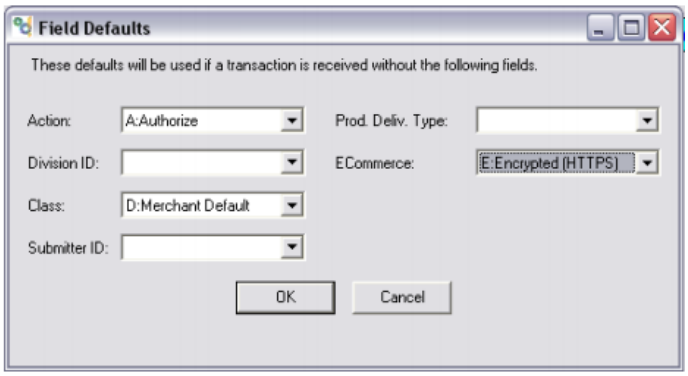
   to return to the Web Request Format screen.

9. Click on a radio button to identify the Delimiter for the items of information in each field in the Preview box. The default delimiter is an ampersand (&).

10. Type a character in the Field Value Separator to change the character that separates fields in the Preview box. The default delimiter is an equal sign (=).

11. Click on

    to view:



This screen lets you select default information for Trevance® to use with the transaction if certain fields are missing.

12. Select the default action that you want Trevance® to use. *The action must always be* Authorize. Every transaction that Trevance® receives with a blank Action field is assumed to be an authorization
13. You may need to change other defaults, such as Division ID, Class (merchant default, MOTO, recurring, E-commerce, or installment), Tender (credit card, purchase card, or check), Submitter ID, Prod. Type (for example, gift certificate or shareware), and ECommerce (channel encrypted, unsecure, or SET). The choices that appear depend upon (a) your processing service and (b) the information you entered when configuring processor settings (specifically, the submitter and division ID information).
14. Click on OK to return to the Web Request Format screen.
15. Under Options, select either or both of the options:
    - URL Encoded prevents the system from confusing ordinary field characters (/, <, and >) with specific URL characters. Some field characters (such as the slash in 10/06) have a very different meaning in a URL.

      When URL Encoded has a check-mark, the system automatically replaces these field characters with the correct URL code. For example, the date 10/06 appears in the Preview box as 10%2F06.

      If you remove the check-mark, the system assumes that the / isn't an ordinary slash; instead, it's treated as a URL character with a URL function.

      The default is a check-mark at URL Encoded.
    - Value is Quoted adds or removes quotation marks from around each value in a field. The default is no check-mark (no quotes).
16. Click on Copy to copy the information in the preview into another application.

You can paste and save the copied information using any text editor. If you ever need to reconstruct the information or send it to someone, the saved file is available. (After you click on the OK button, this information also appears in the configuration report.)

17. Click on

3.6.3 Formatting the Web Response

The Trevance®— web interface returns results in a delimited text format. By default, the delimiter is a pipe (|). You use the Web Response Format screen to define the order in which fields are returned. You can also choose to send back field names.

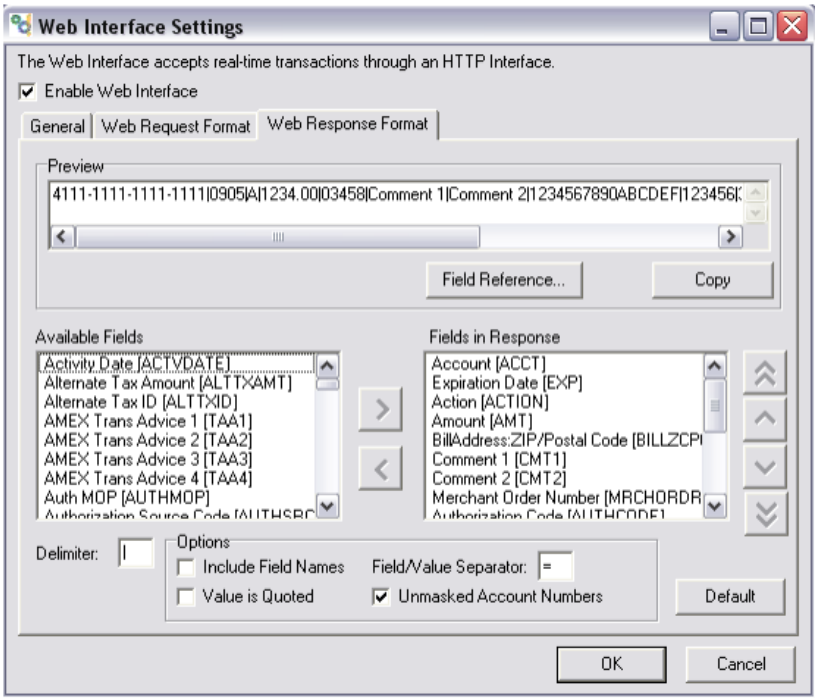
Unlike the Preview on the Web Request Format screen (which merely gives an example of what you can send), the Preview on the Web Response Format screen shows the exact fields that will be returned for each and every transaction.

In addition to specifying fields such as Auth Code, Date, and Response Code, you should ask Trevance® to return the Last Action Succeeded field. This field is always 1 for a successful transaction or 0 for a failed transaction, and is independent of the processing service's response code. It allows you to quickly discover if a transaction succeeded. Auric Systems International recommends including Last Action Succeeded when you format the response (see Step 4 below).

1. Click on Configure.

2. If the server isn't paused, click on *Pause Server to Configure Items Below*.

3. Click on Real Time Web Interface, then the Web Response Format tab to view:



4. There are two main boxes on the Web Response Format screen: Available Fields and Fields in Response. The default fields for export are shown in the Fields in Response box. For example, the Last Action Succeeded field let's you see at a glance if the transaction succeeded (1) or failed (0). You may want to change or add to these fields.
5. To move a field from one box to the other, select the field by clicking on the field name. Then:

Table 3.8: Moving from Boxes

Click on...	*To . . .*
>	Move the selected field into the Fields in Response box

Continued on next page

Table 3.8 – *Continued from previous page*

Click on...	*To . . .*
	Move all the available fields into the Fields in Response box
	Move the selected field into the Available Fields box (that field isn't exported)
	Move all the fields into the Available Fields box (no fields are exported))

6. The first field shown in the Fields in Response box is the first field to appear in the response for each transaction. To change a field's position, select the field by clicking on the field name. Then:

Table 3.9: Changing Fields Position

Click on...	*To . . .*
	To the top spot in the box (the beginning of the record) box
	Up one spot

Continued on next page

Table 3.9 – *Continued from previous page*

Click on...	*To Move Field . . .*
	Down one spot box (that field isn't exported)
	To the bottom spot in the box (the end of the record) box (no fields are exported)

Trevance® arranges each response to show the fields you chose at Step 3, in the order you chose at Step 4.

7. To return all fields to their default position (with the default fields listed in their original order in the FIELDS IN RESPONSE box), click on

8. Type a delimiter in the DELIMITER box. This is the marker that separates each information field in the transaction, as shown in the PREVIEW box. The default delimiter is a pipe (|).

9. Under options you can choose whether to INCLUDE FIELD NAMES and/ or place quotes around the values for each field (VALUE IS QUOTED). To choose these options, click on the box to place a check-mark next to the option. The default is no check-mark.

   You can also change the FIELD SEPARATOR from the default equal sign (=) to any other character.

   Here's how the preview looks with each combination of options (the delimiter is | and the field separator is =):

Table 3.10: Preview

Include Field Name?	*Value is Quoted? . . .*	*Sample Result*
No	No	12345678901234567|10/06
Yes	No	ACCT=12345678901234567|EXP=10/06
No	Yes	"12345678901234567"|"10/06"
Yes	Yes	ACCT="12345678901234567"|EXP="10/06"

10. Click on Default if you change your mind and want to return to the original defaults in all cases.

11. Click on Copy to copy the information in the preview into another application.

    You can paste and save the copied information using any text editor. If you ever need to reconstruct the information or send it to someone, the saved file is available. (After you click on the OK button, this information also appears in the configuration report.)

    Click on OK

3.7 Configuring Directories

Trevance® installs with default directories where it automatically sends and receives the appropriate files. If you decide to change these defaults, you may set up or select any directory, as long as Trevance® has read/write privileges to that directory.

If you are running debit card transactions, you must change the location of the RecoveryLog directory. This directory must be installed on a different drive than Trevance®.The RecoveryLog directory is a copy of Trevance®ś embedded database, which stores

information that the processing service adds to a transaction when it's deposited. You'll need the RecoveryLog if anything happens to the embedded database. Since a hard disk failure is the most likely event to harm the embedded database, you *must* locate the RecoveryLog directory on a different physical hard drive.

If the directories you want to change are on the same machine you're using for configuration, you may change directories in either of two ways, by over-typing or by browsing.

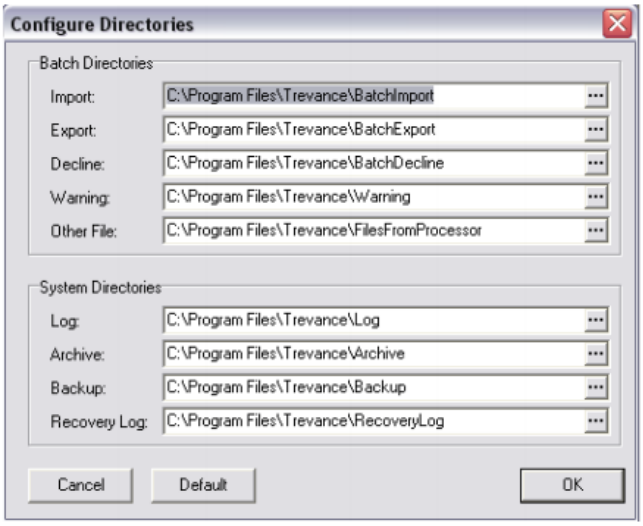
If the Trevance® console and the Trevance® server are running on separate machines, you can't browse. You must change directories by over-typing.

You can also return to the defaults at any time.

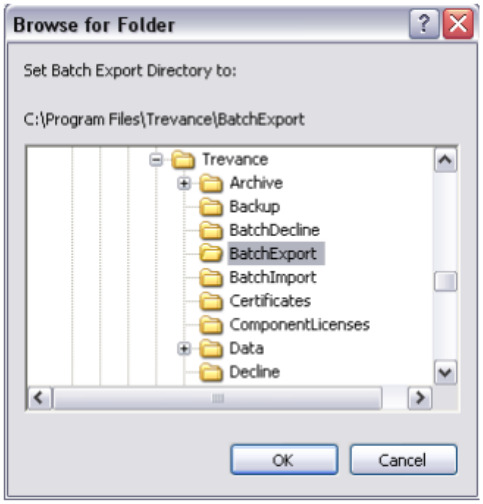
3.7.1 Browsing (for local configuration only)

To change the directories by browsing:

1. Make sure the new directory already exists on your local system, and that you have read/write privileges to that directory.
2. Click on Configure.
3. If the server isn't paused, click on *Pause Server to Configure Items Below*.
4. Click on Directories to view:



5. Click on ... next to the directory you want to change (for example, RecoveryLog) to view a screen like the following:



6. Select your new directory.

7. When you're finished, click on OK

8. Continue changing directories or click on OK again to return to the main Trevance® screen.

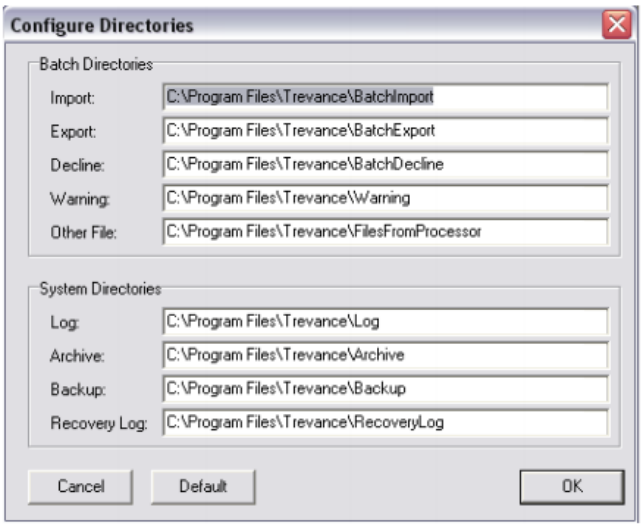
3.7.2 Over-typing (for either local or remote configuration)

To change the directories by over-typing:

1. Click on Configure.

2. If the server isn't paused, click on *Pause Server to Configure Items Below*.

3. Click on Directories to view:



4. Select the name of the directory you want to change (for example, RecoveryLog).
5. Type in the new directory path.
6. Click on

Trevance® automatically creates the new directory, if necessary.

3.7.3 Returning to Defaults

To return to the defaults (the directories in place when you first installed Trevance® click on

If you're running debit card transactions, you must change the default location of RecoveryLog directory so that it's not on the same drive as Trevance®

3.8 Configuring Options

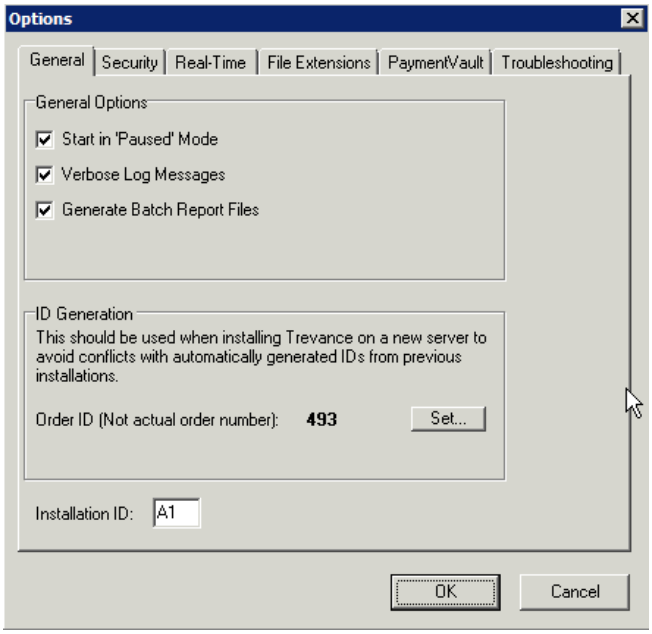
Trevance® lets you decide whether to change the default file extensions.

3.8.1 Changing General Options

Before you can exit Trevance® you must pause it. But by default, when you restart Trevance® it's already working (not paused) and immediately starts processing files. Starting in paused mode is useful when you're working in a fully automated environment and need a chance to clear up data files when servers restart. The general options screen allows you to set up Trevance® to start in paused mode; receive long log messages; and change the current order number.

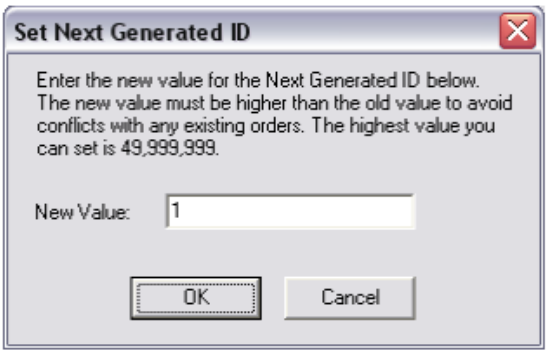
To change the general options:

1. Click on Configure.
2. If necessary, click on *Pause Server to Configure Items Below*.
3. Click on Options.
4. Click on the General tab to view:



5. If you want Trevance® to always start paused (not running), click on the box next to Start in 'Paused' Mode to show a check-mark.
6. If you want long (verbose) log messages, click on the box next to Verbose Log Messages to show a check-mark.

7. If you want to change the current order number, click on Set... to view:


Set Next Generated ID
Enter the new value for the Next Generated ID below. The new value must be higher than the old value to avoid conflicts with any existing orders. The highest value you can set is 49,999,999.
New Value:
1
OK
Cancel

8. In the New Value box, type the number at which automatic number generation should start. Click on OK to return to the General options screen.

9. Click on OK

3.8.2 Selecting a Secure File Deletion Method

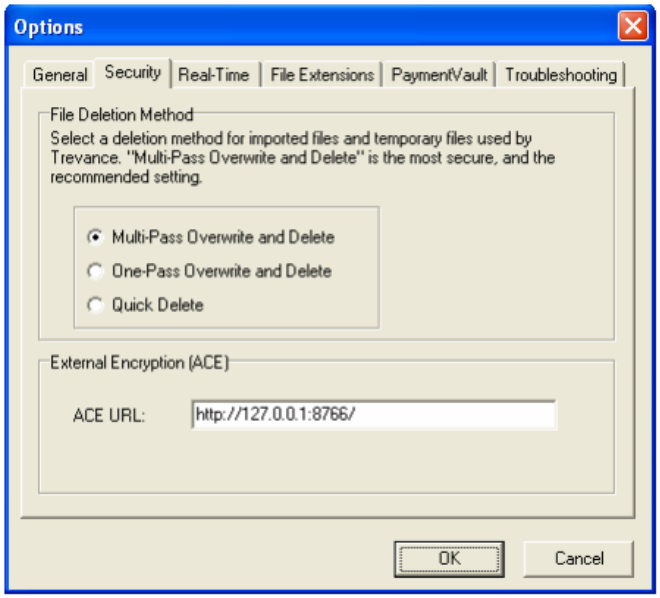
For security, you need to delete the imported files and temporary files that Trevance® uses.

1. Click on Configure.

2. If necessary, click on *Pause Server to Configure Items Below*.

3. Click on Options.

4. Click on the Security tab to view:



5. Select one of the options. The default is Multi-Pass Overwrite and Delete; it is also the most secure option.

6. See ACE chapter for details on the ACE URL setting.

7. Click on

3.8.3 Changing File Extensions

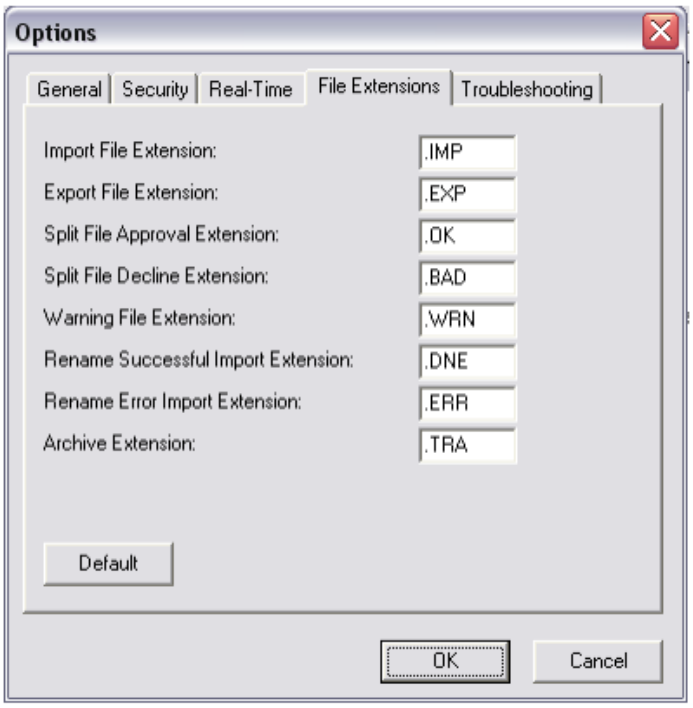
You may change the file extensions that Trevance® uses for import, export, split (approved and declined), warning, done, and error files.

1. Click on Configure.

2. If necessary, click on *Pause Server to Configure Items Below*.

3. Click on Options.

4. Click on the File Extensions tab to view:



5. Type in a new file extension.
   You must assign a *unique* file extension to import files. You will create major problems if, for example, import files and done files have the same file extension. The other files may all use the same extension, if your installation requires that.
6. If you change your mind, you can return to the defaults (the extensions in place after you install Trevance®).
   Click on

7. When you've finished changing the extensions, click on

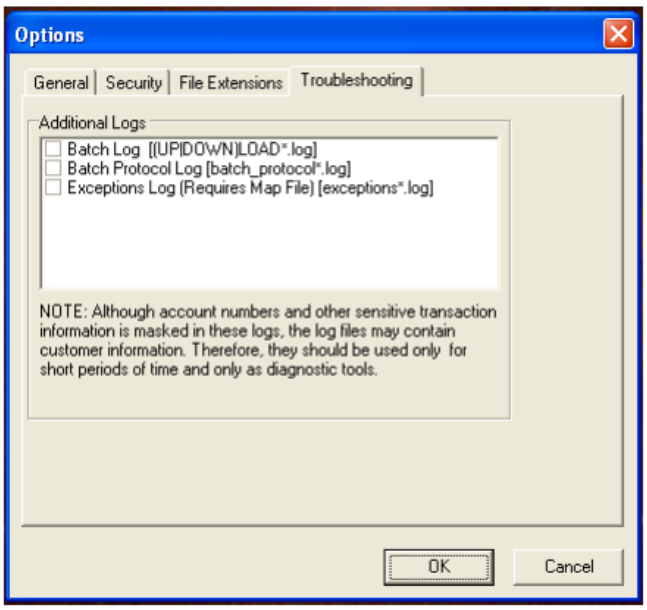
3.8.4 Changing Troubleshooting Options

Trevance® can generate a number of logs that are useful when attempting to troubleshoot problems.

All Trevance® logs are sanitized so that sensitive account and Card Identifier information does not appear in the logs. However, there is still significant sensitive information (customer names and

addresses) in the logs. Plus, if account or Card ID information is passed in incorrect fields (e.g., sending a credit card number in an address field), the information is not sanitized.

1. Click on Configure.
2. If necessary, click on *Pause Server to Configure Items Below*.
3. Click on Options.
4. Click on Troubleshooting to view:


Options
General
Security
File Extensions
Troubleshooting
Additional Logs
Batch Log [(UP|DOWN)LOAD*.log]
Batch Protocol Log [batch_protocol*.log]
Exceptions Log (Requires Map File) [exceptions*.log]
NOTE: Although account numbers and other sensitive transaction information is masked in these logs, the log files may contain customer information. Therefore, they should be used only for short periods of time and only as diagnostic tools.
OK
Cancel

3.8.4.1 Additional Logs

5. Click on the logs you want to create.
6. Click on

   If you chose additional logs in Step 5, the following message appears:

Trevance Console
One or more additional logs are active. Additional logs may contain confidential information (e.g., credit card numbers). Therefore, they should be used only for short periods of time and only as diagnostic tools.
OK

7. Click on OK to save the selected logs to the LOG directory.

3.9 Producing a Configuration Report

The configuration report contains general information about your system and records every configuration decision you made (for example, whether you selected file polling or asked Trevance® to export a division ID with each transaction). This report is available from the Help menu. Auric Systems International recommends that you keep a copy of this report (perhaps even under version control) in case you ever want to duplicate a particular configuration. This configuration report is also used to troubleshoot your system.

The configuration report appears on screen and can be copied into any text or word processing program.

The content of the configuration file is created when you export the configuration report. It *must* remain in .XML format.

Using the configuration file, you can:

- Backup configuration information (export) and then restore it to the same installation (import).
- Copy configuration information from one installation of Trevance® (export) and transport it to another installation (import).

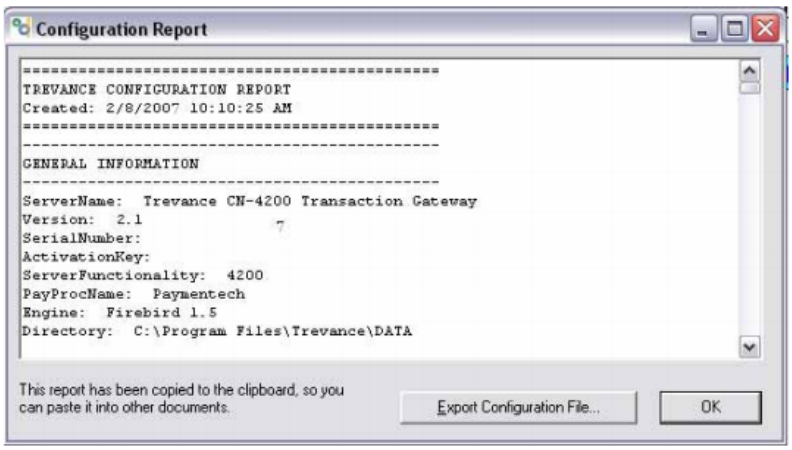
There are several important points to remember when exporting or importing configuration information:

Table 3.11: Importing/Exporting Configuration Information

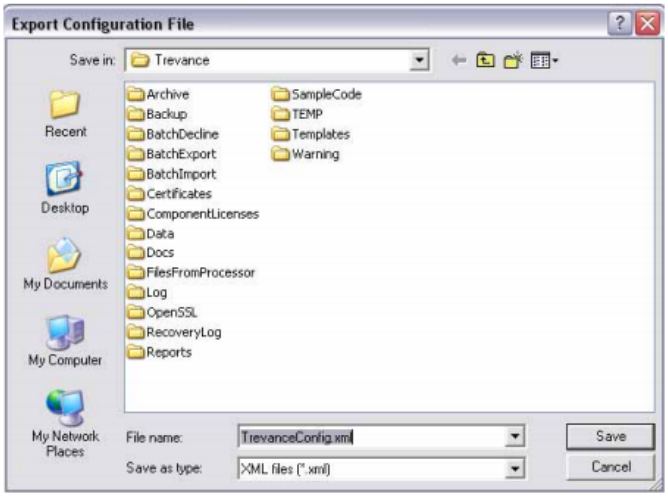
	Format of Information	*Content of Information*	*User*
EXPORT	XML format	Trevance® exports all configuration information except for passwords. (This export file is the only configuration file that Trevance® can import.)	Anyone–Administrators, console users, and web users–can export.
IMPORT	.XML format	Trevance® never imports passwords, run mode, serial number, and activation key. Those four items stay the same. All other configuration information is replaced by the information in the imported file.	Only an administrator can import.

3.9.0.2 View and Export Configuration File

1. Click on Help
2. Click on Configuration Report to view a report like the following:

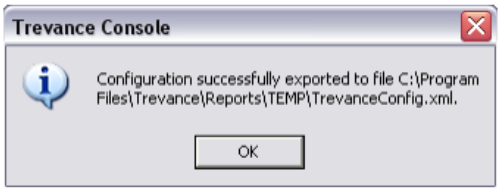


3. To export this report, click on Export Configuration File... to view a screen like the following:



4. You may leave the Save in location and File name as is or change either one. Be sure that the Save as type is always XML files and that the file name always has an .XML extension.

5. Click on Save to view a message like the following:



6. Click on OK to return to the Troubleshooting screen

7. Click on OK

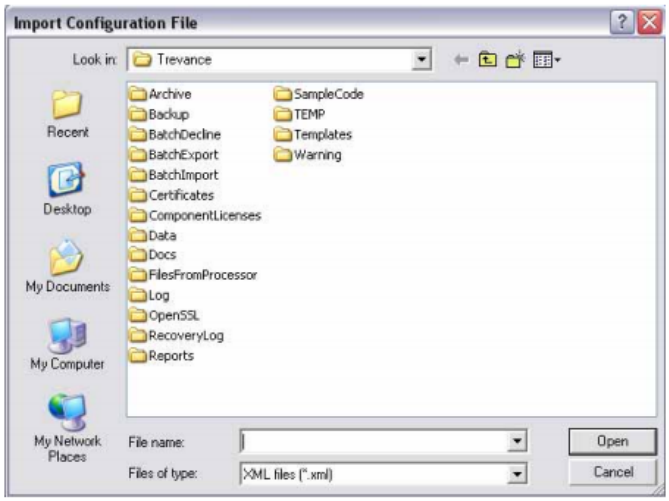
3.9.0.3 Import Configuration File

After you export a Trevance® configuration file (say, from installation A), you may save it as a back up or import it either to the same installation of Trevance® (installation A) or to a completely

different installation (installation B). The imported file replaces *all* the current configuration information in either A or B, except for passwords, run mode, serial number, and activation key.

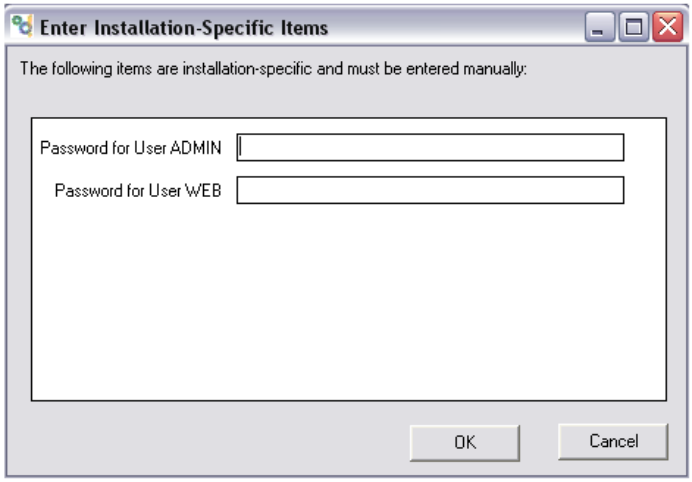
1. Click on the File menu.

2. Click on Import Configuration File to view a screen like the following:



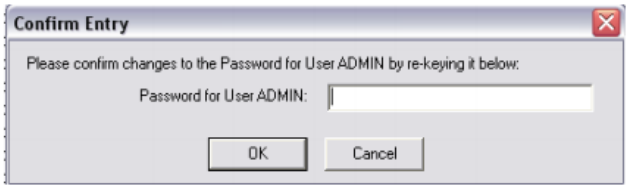
3. Browse to the location of the .XML file you exported. *The only type of file you can import is a .XML file that was exported by Trevance® using the* Export Configuration File *option.*

4. Click on Open to view:



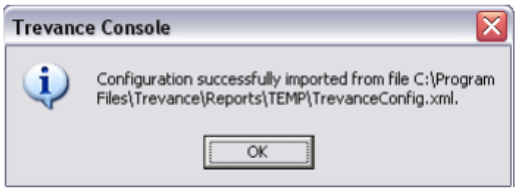
5. Enter the appropriate passwords.

6. Click on OK to view a confirmation message for the passwords.


Confirm Entry
Please confirm changes to the Password for User ADMIN by re-keying it below:
Password for User ADMIN:
OK
Cancel

7. Re-enter your passwords and click on OK each time.

8. Click on OK to view:



3.10 Switching between Versions in Demo Mode

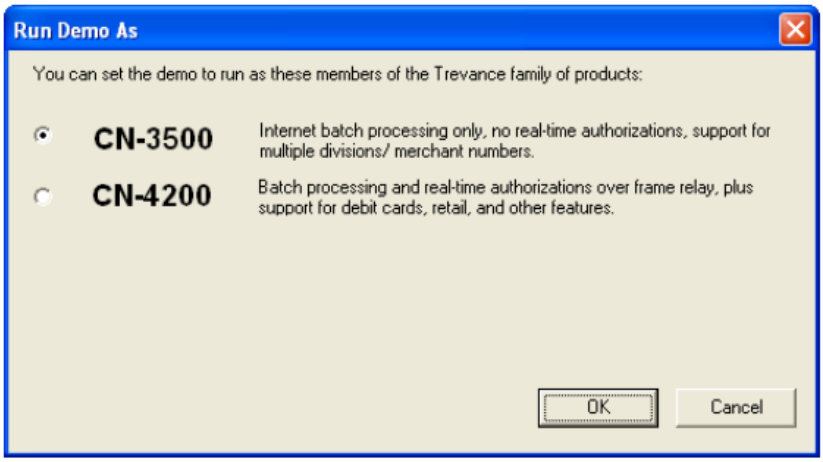
By default Trevance® installs as a CN-3500. In the demo mode of Trevance®, you may switch versions; again, the versions available depend on your processing service.

After you enter the serial number and activation key, you can continue to switch between versions as long as you are in demo mode. Any time that you switch to test or production mode, the system automatically locks into the version of Trevance® that you purchased (for example, CN-4200).

The following procedure assumes your processing service is Chase Paymentech Solutions and you want to switch from CN-3500 to CN-4200.

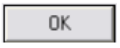
To switch between versions:

1. Click on Configure.
2. If necessary, click on *Pause Server to Configure Items Below*.
3. Click on Run Demo As to view a screen like the following:


Run Demo As
You can set the demo to run as these members of the Trevance family of products:
CN-3500
Internet batch processing only, no real-time authorizations, support for multiple divisions/ merchant numbers.
CN-4200
Batch processing and real-time authorizations over frame relay, plus support for debit cards, retail, and other features.
OK
Cancel

4. Select the version of Trevance® you want to run. In this example, you would click on CN-4200.
5. Click on to view:

Trevance Console
Demo product capabilities modified. THESE CHANGES WILL NOT TAKE PLACE UNTIL TREVANCE IS RESTARTED. Please restart the Trevance Server.
OK

6. Click on 

7. Exit Trevance® , shut down the server, and restart.

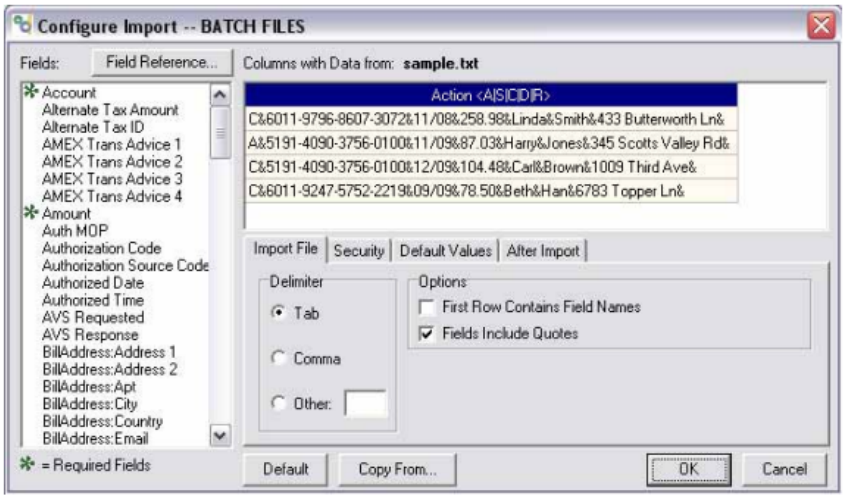
3.11 Working with an Import File That Isn't Typical

So far, this chapter has assumed that your imported text file uses a tab for a delimiter and places quotation marks around each field. But what if it doesn't?

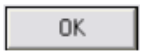
Here's part of a delimited text file that uses an ampersand for a delimiter and omits the quotes:

C&6011-9796-8607-3072&11/08&258.98&Linda&Smith&

When you open this file in the Configure Import screen, it looks like this:



1. In the Other box, type an ampersand (&).

2. Click on the radio button next to Other, and you'll see the proper column layout. Trevance® assigns column headings according to the default field order, which might not match the order of the file.
3. Change field names, replace unassigned column headings with field names, and make any other changes necessary.
4. When the file is correctly formatted for your processing service, click on 

4 Windows® Service

Trevance® runs as either a stand-alone application or as a Windows service. During configuration and testing, you should run Trevance® as an application. Afterwards, you can run Trevance® as a service, with one of the following configurations:

- Local: Both Trevance® and its directories are on the same computer
- Remote: Trevance® is on one computer and at least one of its directories is on another (remote) computer.
- Trevance® automatically installs as an NT service but the service is not activated. To activate the service:
  1. Establish a log-on account for the service, if necessary.
  2. Set up folders.
  3. Set the service up to run as a specific user.
  4. Test the service.

This chapter also describes the recommended NTFS file security configuration, how to uninstall the service, and how to run Trevance® as an application again.

When you run Trevance® as a service, you will not see an icon in the bottom tray on your desktop ().

4.1 Establishing a Log-On Account for the Service

You may need a log-on account if you need special privileges for remote or local configuration. In that case, you must establish the log-on account before you install Trevance® as a service.

4.1.1 All Directories Local

If all your directories (including import, export, archive, and warning) are on the same computer as Trevance® , the service can run as the System Account. If you don't need a special account, the server will log on to the local system account by default.

4.1.2 At Least One Remote Directory

If you place even one directory on a remote computer, you need a user account that serves as the "Log On As...?" account for the service. That user account must have read and write privileges for the directories and the files in the directories. You must create the account on the same computer with Trevance® . The exact procedure changes depending on the operating system for your computer.

The following procedures assume:

- You're running Trevance® as a service.
- The import and export are configured to a remote computer.
- The two computers are peers in a workgroup with no domain users available.
- The user account is called Trevance® (this is an example only; you may name the account anything you like).

4.1.2.1 XP Professional

1. Open User Accounts in the control panel.
2. Click on Create a New Account.
3. Name your new account trevanceservice.
4. Click Next.
5. At Account Type, click on the Computer Administrator radio button. (Administrators have certain rights, including the right to log on as a service.)
6. Your new account is listed under Pick an account to change.
7. At Create a password, type in a password.
8. 2003 Server and 2000 Professional
9. Open Users and Passwords in the control panel.
10. At User Name, type trevanceservice.
11. Click Next.
12. At Password, type in a password; repeat in the Confirm Password box.

13. At Level of Access, click on Other.
14. Scroll down until Administrators appears in the Others box.
15. Click on Finish.

4.1.3 After Establishing the Log-On Account

After you've established the log-on account, you must set up Trevance® to run the server as described in "Run Trevance® As a Service" on page 129. Exit Trevance® then start the service manually.

4.2 Setting Up and Changing Remote Directories

The following procedure is necessary if at least one Trevance® directory is on a remote computer (it isn't necessary for local service).

You must create a user name and password on the computer where your directories are located. This user name and password must be exactly the same as the one you established for the computer where Trevance® is installed (see page 126). Use the same procedure, also.

1. On the computer where Trevance® is installed, open Trevance®
2. Click on Configure
3. Click on *Pause Server to Configure Items Below*.
4. Click on Directories.
5. Set up the UNC path to the folders on the remote machine.
6. Click
7. Click on File.
8. Click on Exit.

To change directories in the future, you must first use your user name and password to log on to the computer where Trevance® is installed.

- If Trevance® is running as a service, stop the service through the Windows Control Panel (that action automatically shuts down Trevance®)
- Do not reboot.
- Re-open Trevance® as an application, make the changes you want, and then pause and exit.
- Restart Trevance® as a service.
- Switching between Application and Service Trevance® automatically installs as a service. You can use the command line to remove the Windows service (that is, to run Trevance® as an application) and also to re-install Trevance® as a service.

Table 4.1: Trevance® as a Service

Action	*Command Line*
Remove the service trevance	UNINSTALL
Remove the service trevance	INSTALL

After Trevance® is installed as a service - either automatically during installation or manually using the command line - you must go to the Windows control panel (Administrative Tools, Services) to actually start running the service. You also need to stop running the service before you can use run Trevance® as an application. These procedures are described next.

1. Run Trevance® As a Service
2. You've just installed or re-installed Trevance® as a service and now want to run it as a service:
3. Browse to the Windows services control panel and double click on Trevance®
4. Browse to the Windows control panel.
5. Click on Administrative Tools, then double click on Services.

6. Double click on Trevance® to view a screen like the following:
7. Set the Startup Type to Automatic.
8. Click on the Log On tab to view a screen like the following:

At This Account, type in the specific account and password under which Trevance® will run. Do not run it under the Local System Account. If you do, Trevance® will never find the necessary passphrase, which is stored in the user account.

1. Click on
2. Restart Trevance®
3. Run Trevance® as an application
4. Suppose you've been running Trevance® as a service and now want to run it as an application:
5. Browse to the Windows control panel.
6. Click on Administrative Tools, then double click on Services.
7. Double click on Trevance® to view a screen like the following:
8. At Service Status, click on the Stop button.
9. Set the Startup Type to Manual.
10. Click on
11. Restart Trevance®

4.2.1 Testing the Service

Before you test the service, you must start the Trevance® Console and connect to the service.

- To test the service, check if Trevance® is processing transactions.
- Click on Trevance® 's Log tab.
- Place a file with an .IMP extension in your BATCHIMPORT directory.
- You should see the transactions being imported, processed, and exported.

- Afterwards, you might also check the BATCHIMPORT folder to confirm that Trevance® renamed the .IMP file with .DNE extension or deleted it.
- Recommended NTFS File Security Configuration

Auric Systems International recommends that you provide the following privileges for Trevance® directories, subdirectories, and files: Type of Privileges Trevance® Directory Execute Trevance® directory Read/Write Trevance.ini file Read/Write (but not execute) Archive, BatchDecline, BatchExport, BatchImport, Data, Decline, Export, Import, Log, Warning (both the directories and all their subdirectories)

5 Testing and Activating Trevance®

This chapter describes how to test your Trevance® configuration in demo mode, enter your serial number and activation key, and then switch between the test and production Trevance® .

Before you try out Trevance® in the production mode and actually process real transactions, you should conduct three configuration tests:

- A web interface test in demo mode
- A test of real-time and batch imports and exports in demo mode
- A test of your connection with the processing service in test mode

Before you test your connection with the processing service in test mode, you must:

- Log in as an administrator (not as the default ADMIN user), as described in Chapter 4.
- Set the server pass key, as described in Chapter 4.
- Enter your serial number and activation key, as described in this chapter.

When Trevance® is in test mode, your processing service receives transactions but doesn't actually process them.

5.1 Testing Your Configuration in Demo Mode

This test has two parts: a test of the web interface and a test of the import and export configuration.

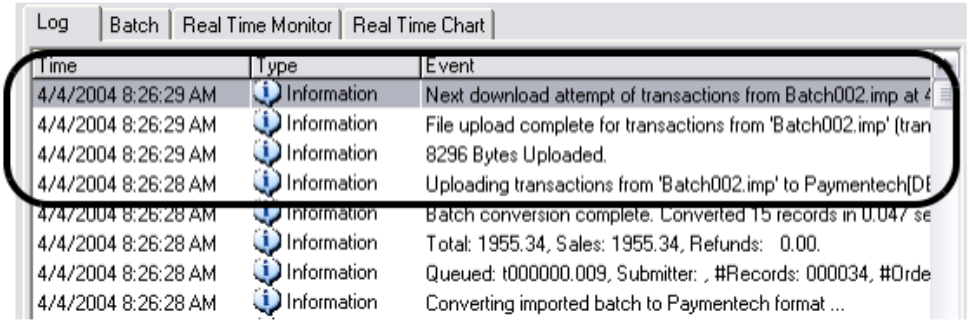
5.1.1 Testing Your Batch Import and Export Configuration

It's best to use the demo mode of Trevance® when testing your import and export configuration. Otherwise, you'll actually sub-

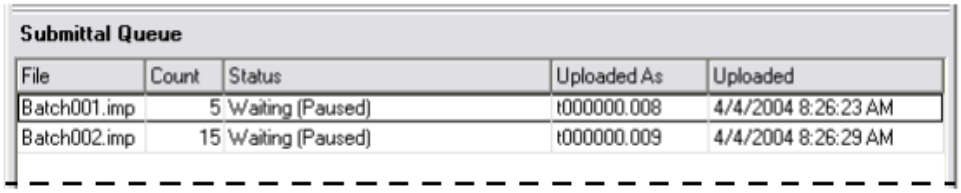
mit the test file to your processing service. You need a sample file with a .IMP extension, preferably a copy of the same file you used during import configuration.

In the following procedure, CreditCards.txt has been copied and renamed to *Batch002.imp*. This is a batch file.

1. Pause Trevance® while you prepare a batch test file: It must have a .IMP extension and must be located in the BATCHIMPORT directory.
2. When your file is ready, click on Server.
3. Click on Resume.
4. Check the on-screen log to see if it records an import. For example:

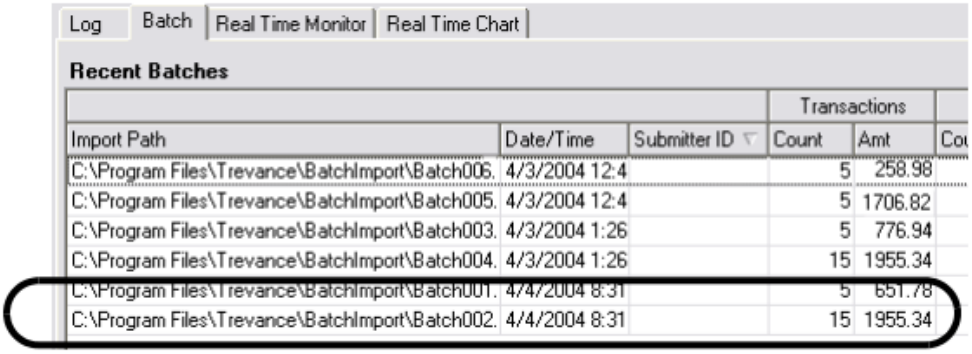


5. Click on Server.
6. Click on Pause.
7. Click on the Batch tab.
8. Look at the Submittal Queue to see if the file is on the queue. For example:

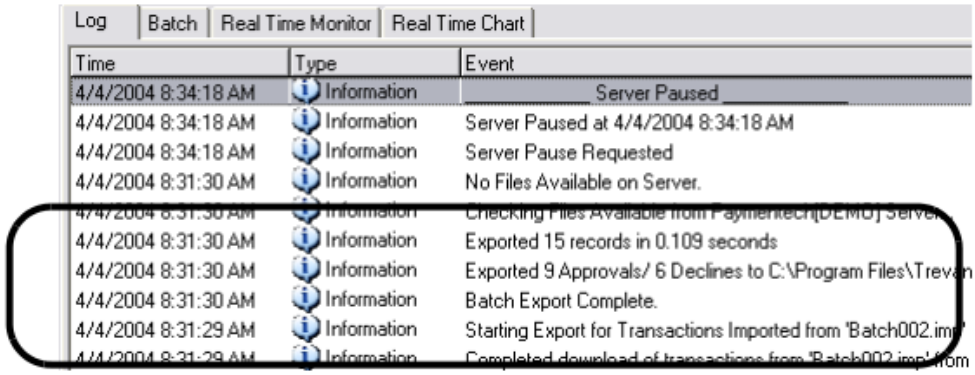


9. Click on Server.

10. Click on Resume.
11. When the file is processed and exported, the file disappears from the queue and appears on the Recent Batches list:



12. Also, the on-screen log contains information like the following:


Log
Batch
Real Time Monitor
Real Time Chart
Time
Type
Event
4/4/2004 8:34:18 AM Information Server Paused
4/4/2004 8:34:18 AM Information Server Paused at 4/4/2004 8:34:18 AM
4/4/2004 8:34:18 AM Information Server Pause Requested
4/4/2004 8:31:30 AM Information No Files Available on Server.
4/4/2004 8:31:30 AM Information Exported 15 records in 0.109 seconds
4/4/2004 8:31:30 AM Information Exported 9 Approvals/ 6 Declines to C:\Program Files\Trev
4/4/2004 8:31:30 AM Information Batch Export Complete.
4/4/2004 8:31:29 AM Information Starting Export for Transactions Imported from 'Batch002.im

13. Check the following:
    - Did you configure Trevance® to place all transactions (approved and declined) in the same BATCHEXPORT file? If so, use Windows Explorer to check that the BATCHEXPORT directory contains a file with a .EXP extension.

      In this example, the import file was named *Batch002.imp.* Therefore, the BATCHEXPORT directory should have a file named *Batch002 .exp.*
    - Did you configure Trevance® to split approvals from declines at export? If so, use Windows Explorer to

check that the BATCHEXPORT directory contains a file with a .OK extension (*Batch002.ok*). Also, the DECLINE directory may contain a file with a .BAD extension (*Batch002.bad*), if your processing service declined at least one transaction.

- Check that improperly formatted batch transactions appear in two directories. They always appear in the WARNING directory (in this example, the file is named *Batch002.WRN*). They should also appear in the BATCHEXPORT directory. If Trevance® is configured to split approved transactions from declined, then declined transactions should appear in the DECLINE directory.

14. Did you configure Trevance® to create a done file (rather than deleting the .IMP file)? If so, the BATCHIMPORT directory should contain a file with a .DNE extension (for example, *Batch002.DNE*).

15. View any of the files with your text editor or word processor, to check the content.

16. If Trevance® doesn't act as expected or if it rejects your file:

- Check the extensions on your files. Make sure your import file doesn't have a double extension. If you changed the default extension for any file, make sure you didn't duplicate an existing extension. Also make sure that your application recognizes the new names.

- Check your import configuration. Make sure you configured imports to match the test file.

- Check your export configuration.

- Check your directory configuration. If you changed the defaults, make sure your application and Trevance® know where to send and find files.

- Make sure you're looking in the correct directories for batches and for real-time web transactions.

5.1.2 Testing the Web Interface

A sample HTML page (WebIntefaceTest.html) is installed in Trevance® 's SampleHTML directory. This test page allows you to send transactions to Trevance® directly from your web browser and see how the interface should work. It is *not for production use.*

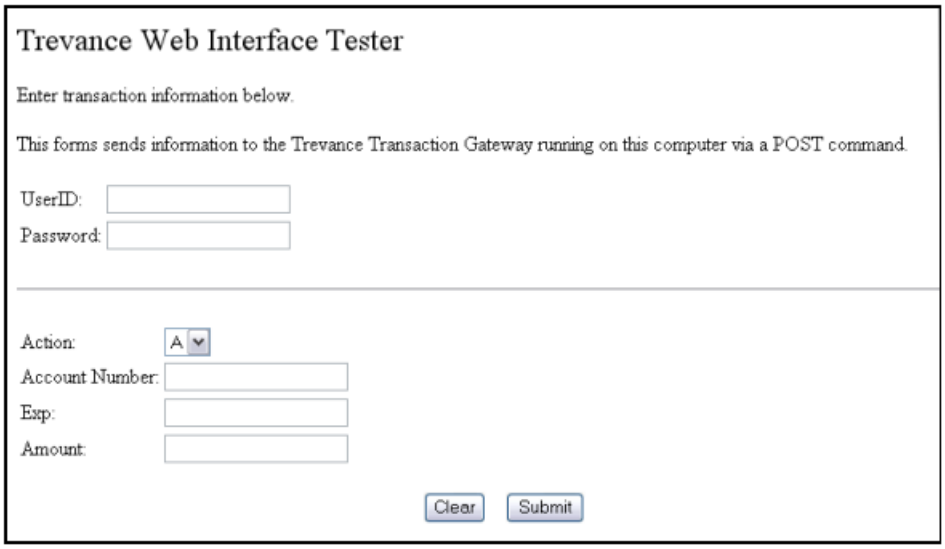
Before you begin the test, make sure that:

- Trevance® is running on a local machine.
- The server port is set at the default value of 8004.
- The Web Request Format screen specifies the default field/value separator (=) and delimiter (&).

To conduct the test:

1. Make sure Trevance® isn't paused. If necessary, click on Server, then Resume.
2. Right click on

3. Click on Explore.
4. Click on Program Files.
5. Click on the Trevance® directory, then SampleCode, and then HTML.
6. Open the WebInterfaceTest.html file to view:



7. At UserID, enter the name of a web user (the default is WEB).

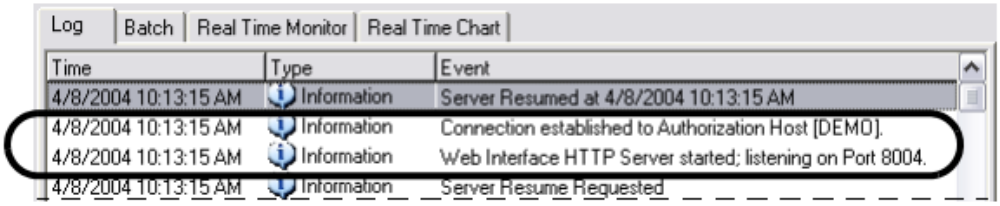
8. At Password, enter the password for that web user (the default is WEBPW).

9. The Action must be A, for authorization.

10. Fill in the account number, expiration date, and amount of the transaction.

11. Click on

12. You'll receive a message through your browser that confirms whether the web interface worked. You should also see a message like the following on the Trevance® Log screen:



5.2 Entering Your Serial Number and Activation Key

After you enter the serial number and activation key, you can switch Trevance® from demo mode to test or production (and back again). You should keep Trevance® in demo mode until you've tested your configuration and it works smoothly. You should switch to production mode only *after* you finish testing your configuration. Thereafter, you can switch between all three modes whenever you like.

You must pause Trevance® before you're allowed to enter the serial number and activation key. Trevance® remains paused after you switch modes, until you tell it to resume.

Here are the differences between demo, test, and production mode:

Table 5.1: Demo Test Production Mode Differences

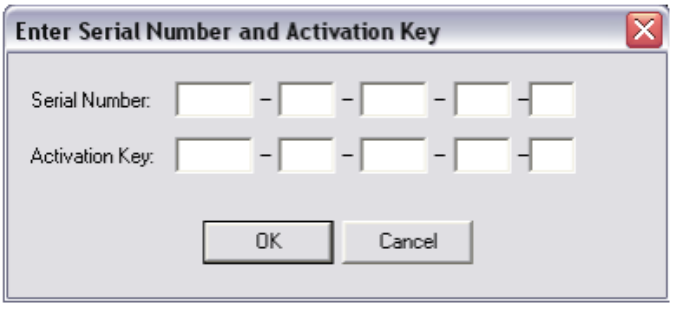
	Demo	*Test*	*Production*
Transactions are sent to processing service?	No	Yes	Yes
Transactions are really processed (money is exchanged)?	No	No	Yes
Message appears on the screen?	DEMO	TEST	Production

*If you configured your processor settings so that the processor tests transactions only, you'll see **TEST** on your screen, even though Trevance® is in production mode. Transactions sent to the processing service won't be processed until you change that setting.

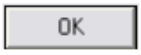
Trevance® remembers the configuration you set up in the demo mode and uses it in the test/production mode.

5.2.1 Switching from Demo Mode to Test Mode for the First Time

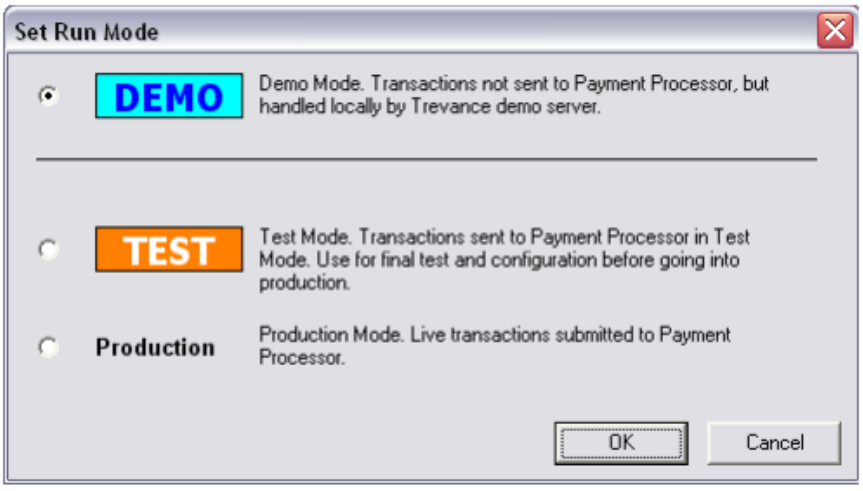
1. Click on Configure.
2. If necessary, click on *Pause Server to Configure Items Below*.
   You must pause Trevance® before you're allowed to enter the serial number and activation key.
3. Click on Serial Number and Activation Key to view:



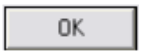
   Fill in your serial number and your activation key. (After you bought Trevance® Auric Systems International e-mailed these numbers to you.)

4. Click on 

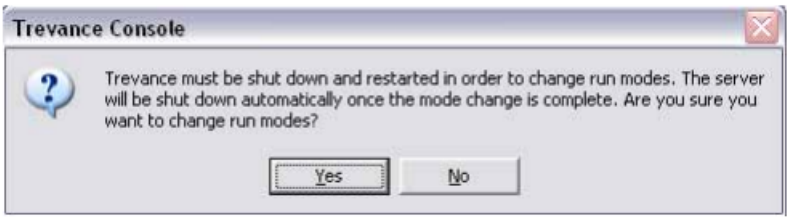
5. Click on Configure.
6. Click on Set Run Mode to view:


Set Run Mode
DEMO
Demo Mode. Transactions not sent to Payment Processor, but handled locally by Trevance demo server.
TEST
Test Mode. Transactions sent to Payment Processor in Test Mode. Use for final test and configuration before going into production.
Production
Production Mode. Live transactions submitted to Payment Processor.
OK
Cancel

7. Click on the radio button for the test mode.

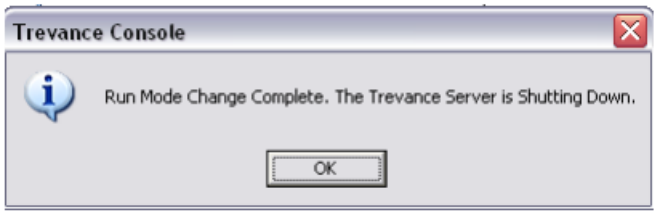
8. Click on 

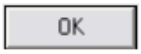
to view:


Trevance Console
Trevance must be shut down and restarted in order to change run modes. The server will be shut down automatically once the mode change is complete. Are you sure you want to change run modes?
Yes
No

9. Click on

to view:



10. Click on 

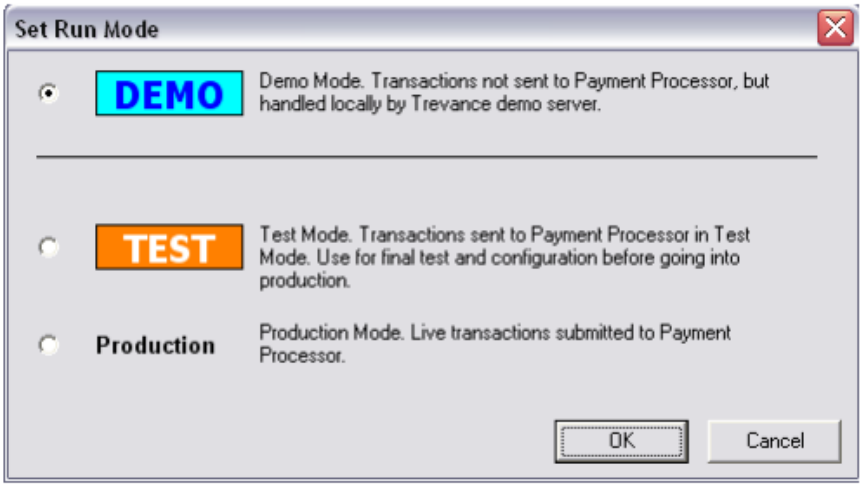
11. In the new mode, Trevance® is paused. If you want to begin processing transactions in test mode, you must resume Trevance® .

12. Click on Configure, then on *Resume Server when Configuration Complete*.

5.2.2 Switching between Modes

You can switch back and forth between modes at any time:

1. Click on Set Run Mode to view:


Set Run Mode
DEMO
Demo Mode. Transactions not sent to Payment Processor, but handled locally by Trevance demo server.
TEST
Test Mode. Transactions sent to Payment Processor in Test Mode. Use for final test and configuration before going into production.
Production
Production Mode. Live transactions submitted to Payment Processor.
OK
Cancel

2. Click on the radio button for the mode you want: demo, test, or production.

3. In the new mode, Trevance® is paused. If you want to begin processing transactions, you must resume Trevance® .

   Click on Configure, then on *Resume Server when Configuration Complete*.

5.3 Testing Your Configuration in Test Mode

Make sure that you have logged in as an administrator (not as the default ADMIN user), that you have set the server passphrase, and that you have entered the serial number and activation key. Trevance® won't change to test mode until those tasks are completed.

Contact your processing service and alert them that you are about to test transactions. Repeat the test that you conducted in demo mode. At the end of the test, contact your processing service to make sure the transactions actually arrived.

Before you switch to production mode, make sure that:

- You have no .IMP files waiting in the BATCHIMPORT directory, especially dummy .IMP files created solely for configuration and testing.
- Your processor settings allow for live transactions.

If you change Trevance® to production mode, but the word TEST still appears on the upper right hand corner of the screen, you must re-configure processor settings. See "Part II. Your Processing Service? (starting on page 193).

6 Understanding Trevance®

Trevance® makes things simple.

Trevance® takes transactions as simple text files (or web messages), automatically translates them into your processing service's detailed specifications, and sends them to the processing service.

The processing service sends the results back to Trevance® , and Trevance® decodes them - it puts the processing service's detailed specification into simple text files (or web responses). Trevance® gives you the results that you want to see.

It's that simple.

Start by processing credit cards, then move on to electronic checks by adding one or two fields. You don't need to understand an entire new subsection of your processing service's specifications. Trevance® does that for you. Trevance® contains all the tools required for communicating with your processing service-they're already built in.

This chapter explains how Trevance® handles transactions. It defines important terms used throughout this manual and describes the main Trevance® screen.

In the next chapter, you'll use this information to set up Trevance® so that it receives, formats, and sends transactions in the way you want.

6.1 What Does Trevance® Do?

Trevance® moves transactions from your system to your processing service, and back again. These transactions can move either through the high-volume batch interface or through the high-speed real-time interface (currently, authorization only).

The high-volume batch interface uses simple tab or comma delimited text files. For batch files, Trevance® requires an external application that can store transactions in a delimited text file. The high-speed real-time interface uses standard web protocols.

6.1.1 Batch Transactions

Trevance® accepts batches of transactions from your external application, submits the transactions to your processing service, and exports the processed transactions back to your external application. The transactions must be sent in a delimited text file with a .IMP extension.

A batch file contains one or more authorization, sale/conditional deposit, deposit, or refund/credit transactions. Here's what happens:

1. The external application creates a delimited text file (.IMP) containing the records for any number of transactions (from one transaction to several hundred thousand).

2. The external application places that file in Trevance® 's BATCHIMPORT directory.

3. Trevance® receives (*imports*) the text file from the BATCHIMPORT directory and stores all the records in its own database.

   If Trevance® detects any problems with a record, it still imports the record; but a copy of the record and a warning message are placed in the WARNING directory.

   Depending on how you configured Trevance® to handle imports, it either deletes the original .IMP file or changes its extension to .DNE immediately after the file has been successfully loaded into the Trevance® database.

4. Trevance® sends all transactions to your processing service.

5. The processing service processes the transactions; authorizes, approves, or declines each one; and sends a response back to Trevance® .

6. Trevance® updates its database with the information received from your processing service. It then formats the updated transaction records to match the requirements of your external application.

7. Depending on how you configured Trevance® to handle exports, one of the following occurs:

- Trevance® places all transactions (approved and declined) in a .EXP file. The file is stored in the BATCHEXPORT directory.

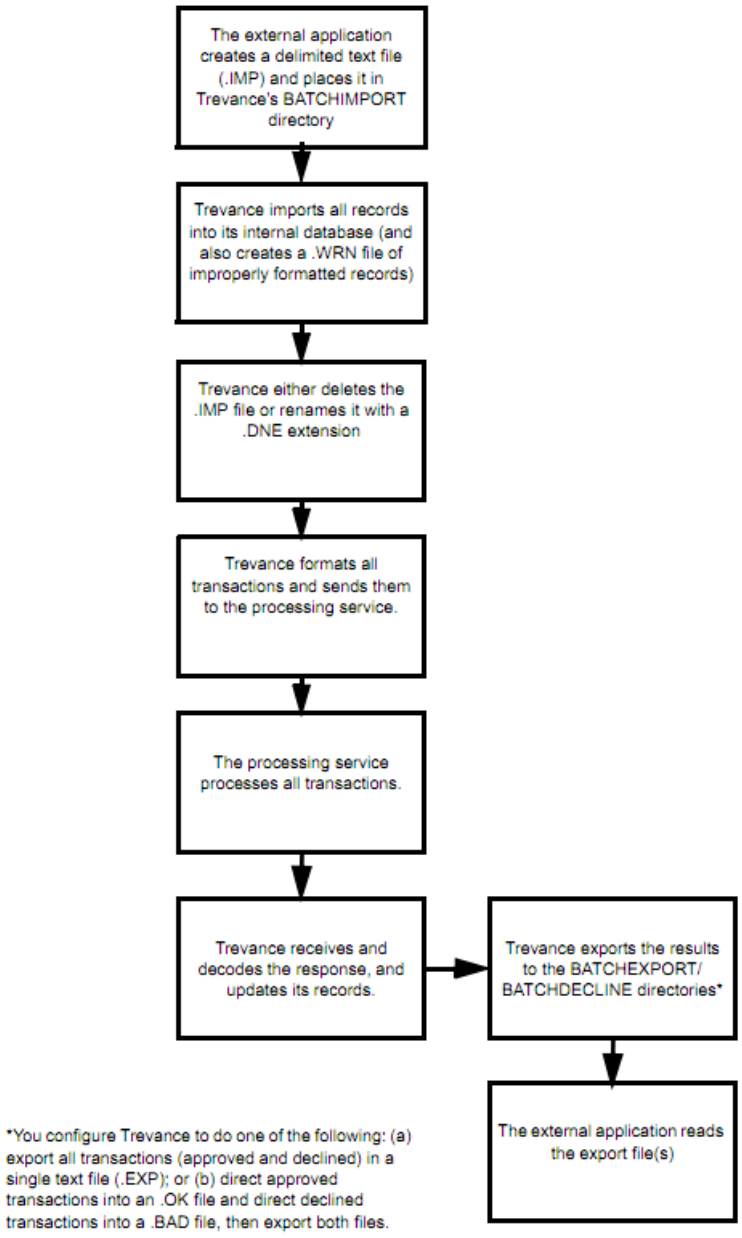
- Trevance® splits approved transactions from declined transactions.

  The declined transactions are placed in a file with a .BAD extension (along with an indication of why they failed). That file is stored in the BATCHDECLINE directory.

  The approved transactions are placed in a file with a .OK extension. That file is stored in the BATCHEXPORT directory.

8. The external application reads the exported file(s).

Trevance® automatically keeps importing, submitting, and exporting until you tell it to pause or exit. You can use any text editor to view any file (including .DNE, .EXP, .BAD, and .OK). The following flow chart describes how Trevance® handles one file. In reality, Trevance® handles many real-time and batch transactions at the same time. It simultaneously imports one file, submits another file, and exports yet another file.


The external application creates a delimited text file (.IMP) and places it in Trevance's BATCHIMPORT directory
Trevance imports all records into its internal database (and also creates a .WRN file of improperly formatted records)
Trevance either deletes the .IMP file or renames it with a .DNE extension
Trevance formats all transactions and sends them to the processing service.
The processing service processes all transactions.
Trevance receives and decodes the response, and updates its records.
Trevance exports the results to the BATCHEXPORT/ BATCHDECLINE directories*
The external application reads the export file(s)
*You configure Trevance to do one of the following: (a) export all transactions (approved and declined) in a single text file (.EXP); or (b) direct approved transactions into an .OK file and direct declined transactions into a .BAD file, then export both files.

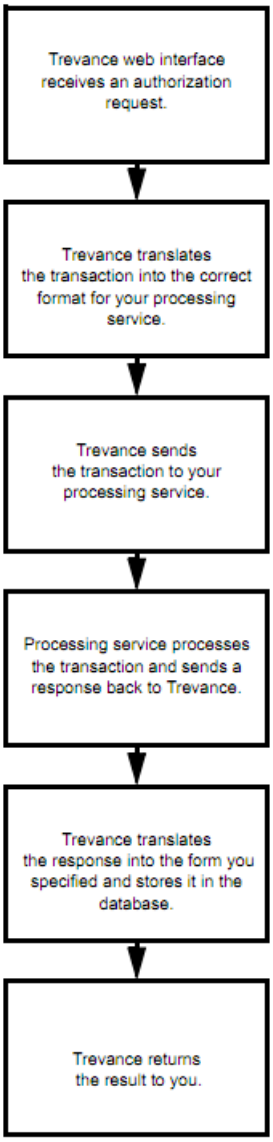
6.1.1.1 Real-Time Web Interface Transactions

Trevance® has a built-in web server for accepting real-time authorization transactions. Any external application (a web site shop-

ping cart, an order entry program, a telemarketing IVR system) can talk to Trevance® if it can create a standard HTTP POST web request. Your application can be written in any language: PHP, Python, Perl, Java, ASP.NET, and so on.

Even though Trevance® uses a web interface, your application doesn't have to be web-based. Almost all computer languages today, from Visual BASIC to Java, know how to talk with web sites. This means that your phone system, your accounting system, your Oracle database-just about anything can talk to Trevance® 's web interface.

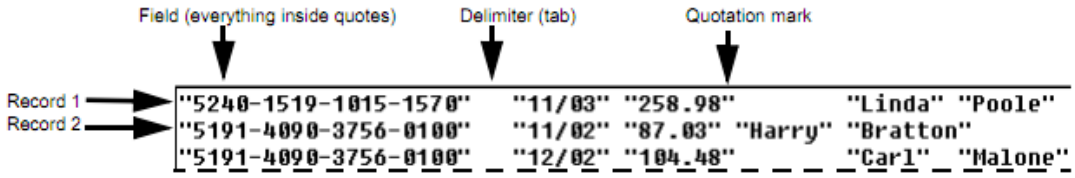
The following flow chart describes how Trevance® handles an authorization transaction using the web interface. Trevance® CN-4200 can handle up to thirty of these transactions per second.


Trevance web interface receives an authorization request.
Trevance translates the transaction into the correct format for your processing service.
Trevance sends the transaction to your processing service.
Processing service processes the transaction and sends a response back to Trevance.
Trevance translates the response into the form you specified and stores it in the database.
Trevance returns the result to you.

6.2 Understanding Delimited Text Files

The external application sends transactions in a delimited text file. The file may contain information about one transaction or thousands.

Each single transaction is called a record; for example, "Record 1" below shows a sale transaction of $258.98 to credit card number 5240-1519-1015-1570, which has an expiration date of November 2003. Each item of information within the record is a field; for example, the amount of the sale ($258.98) is one field and the expiration date of the credit card (11/03) is another field. Each field is separated by a delimiter (usually, a tab or comma) and is usually surrounded by quotes. A typical delimited text file looks like this:



You set up Trevance® 's batch import files (including delimiter and types of fields) to match the requirements of your processing service. You also set up the batch export files to match the requirements of your external application. Once you set up these formats, Trevance® automatically applies them.

Auric Systems International recommends using a tab as the delimiter – *not a comma* – because commas frequently appear in name and address fields. When you use a tab delimiter, you don't have to put quotes around each field.

6.3 Understanding Trevance® Terms

The following definitions appear in alphabetical order. They include answers to questions you may have about the way Trevance® works. For example, if you'd like an explanation of all file extensions, see "File directories and extensions" below.

6.3.0.2 Actions

The following table lists:

- The actions that Trevance® supports
- The standard Trevance® abbreviation for the action

The table also includes a column where you can write the term your processing service uses for the action. For example, a Refund/Credit authorization might be called a "refund" by your processing service.

Table 6.1: Terms

Import Action	*Abbreviation*	*Term Used by Your Processing Service*
Authorization	A	
Sale or Conditional Deposit	S or C	
Deposit	D	
Refund/Credit	R	

6.3.0.3 Activity log

Trevance® tracks real-time transactions and batch transactions that are processed by your processing service and keeps the information in a daily activity log. The log includes information about the amount and type of each transaction and similar details (depending on the processing service). The activity log is stored in the internal data base and automatically exported daily. It can also be exported using the Archive menu. This activity log file is *not* the same as the .LOG file in the LOG directory (see "Log file" below).

6.3.0.4 Archive

Trevance® maintains an activity log that tracks processed transactions. You can export the activity log to a delimited text file with a .TRA extension in the ARCHIVE directory. One file stores information about batch transactions, one is for batch summaries, and the third is for web interface transactions. You can import these files into a spreadsheet or database for reporting or analysis.

6.3.0.5 Batch transactions

Batches contain one or more transactions. The transactions can be authorizations, deposits, sales, and/or refunds. The transactions come from an application (such as an order entry application) that is capable of reading and writing delimited text files. The application doesn't have to be running on the same computer as Trevance® ; it may not even be a Windows application. Any application capable of creating a delimited text file can transactions to Trevance® .

6.3.0.6 Control files

Control files allow external batch or scripting applications to control when and how Trevance® is running. For example, you might configure Trevance® to always start paused–running, but not processing transactions. Then, when all external applications are fully operational, they can send a control file to the Trevance® BATCHIMPORT directory to tell Trevance® to resume working (ONNOW.CN!). If Trevance® is working and the external application needs to pause it (for system maintenance, say), it sends an OFFNOW.CN! file. Trevance® automatically deletes these files after they are processed.

6.3.0.7 Directories

For a list of Trevance® 's default directories and the types of files they contain, see "File directories and extensions" below.

6.3.1 Done files

As soon as Trevance® finishes importing a file into its database (see "Import file and directory" below), it either deletes the file or saves it with an extension of .DNE for *done*. During configuration, you decide whether Trevance® creates a done file.

6.3.2 Export file and directory

The export directory for batch transactions is BATCHEXPORT. Here Trevance® stores files that it exports to your external application.

After the processing service processes the transactions, it sends the results to Trevance® . Trevance® updates its database with this information, then prepares the processed transactions for export in a delimited text file.

Trevance® remembers the name of the import file that contained the original transactions. It places the processed transactions in a delimited text file with the same name; only the extension changes. For example, transactions imported from a file named ABC.IMP are exported to a file named ABC.EXP.

You configure Trevance® to prepare the export file in one of two ways:

- Either it places approved and declined transactions in one file (.EXP)
- Or it places approved transactions in one file (.OK) and declined transactions in another file (.BAD). Then it exports both files. The .BAD file lets you quickly find transactions that need follow-up action, without searching a large .EXP file for a few declined records.

By default, Trevance® does not split approvals from declines.

6.3.2.1 File directories and extensions

Trevance® processes many delimited text files for batch transactions (including bad, done, export, import, and okay files). Information on batch transactions appears in the archive files. Throughout this manual, it's assumed that files are being stored in the

default directories, under the default file extensions. (For information on changing the defaults, see Chapter 4.) The following table defines the default file extensions and directories:

Table 6.2: Default File Extensions

Extension	*Type of File*	*Found in This Directory . . .*
.BAD	Export file containing declined batch transactions (approved transactions are in the .OK file)	BATCHDECLINE (batch transactions)
.CN!	Control file	
.DNE	Import file of batch transactions as received from an external application, except that critical information is masked (alternatively, Trevance® deletes the entire import file after import).	BATCHIMPORT (batch transactions)
.ERR	Error file created if the import procedure fails for some reason; for example, if you changed a directory name using Windows Explorer instead of Trevance® 's Configure menu	BATCHIMPORT (batch transactions)
.EXP	File containing approved and declined batch transactions; the external application reads this file	BATCHEXPORT (batch transactions)
.IMP	File of batch transactions received from an external application; Trevance® reads this file	BATCHIMPORT (batch transactions) (until Trevance® automatically deletes it or changes the extension to .DNE)
.LOG	Log file recording Trevance® operations	LOG

Continued on next page

Table 6.2 – *Continued from previous page*

Extension	*Type of File*	*Found in This Directory . . .*
.OK	Export file containing only approved batch transactions (declines are stored in the .BAD file)	BATCHEXPORT (batch transactions)
.TRA	Archive file containing information on batch and real-time web interface transactions	ARCHIVE (includes BATCH, BATCHSUMMAR, and REALTIME subdirectories)
.WRN	File containing copies of imported batch transactions that were improperly formatted	WARNING

6.3.2.2 File names

Trevance® remembers the name of the import file and uses this name for all other files; only the extension changes. For example, the import file ABC.IMP becomes ABC.EXP, ABC.BAD, ABC.OK, and so on. If there is already a file with the same name in the same directory, Trevance® automatically adds a number to the file name to make it unique. For example:

- ABC.DNE
- ABC_001.DNE
- ABC_002.DNE

This numbering process continues for over two billion files (ABC_2147483647.DNE). If you somehow exceed this number, a warning message appears. However, to avoid the problem, either give your import files unique names or regularly back up (and then clear) your BATCHIMPORT directories.

6.3.2.3 Import file and directory

The external application places a delimited text file (.IMP) in Trevance® 's BATCHIMPORT directory (for batch transactions).

Trevance® stores the contents of this file in its internal database and submits the transactions to your processing service. (You can configure Trevance® to either delete the original .IMP file or save it with a .DNE extension.)

By default, Trevance® looks in the BATCHIMPORT directory for the delimited text files. The import directories can be on a remote machine or file server.

6.3.2.4 Log file

Trevance® keeps a record of its own operations each day in a log file (a basic ASCII text file with the extension .LOG, which it stores in the LOG directory). This file tracks such events as pause, resume, import, and export. A new file is created each day. The Log screen shows the 200 most recent events. (This is not the same as the activity log.)

6.3.2.5 Real time

Trevance® processes real-time transactions through the web interface. Each transaction is processed as soon as it is received.

6.3.2.6 Recovery log

The recovery log is generated when you process a debit card (either PIN-based or PINless). It contains information about a debit card transaction that must be remembered between the transaction's authorization and its capture. The recovery log is a backup of information stored in the Trevance® internal database. This copy is maintained for redundancy. For protection, you should keep the recovery log and Trevance® on different hard drives and back up the recovery log nightly.

6.3.2.7 Warning file

As part of the batch import process, Trevance® checks for transaction records with formatting errors or missing required information. Trevance® writes an entry to the log file and on the Log screen. It saves the records in a warning file (a basic ASCII text

file with the extension .WRN) and stores them in the WARNING directory. The records also go to your processing service, which either accepts or declines them. They're then treated like any other export.

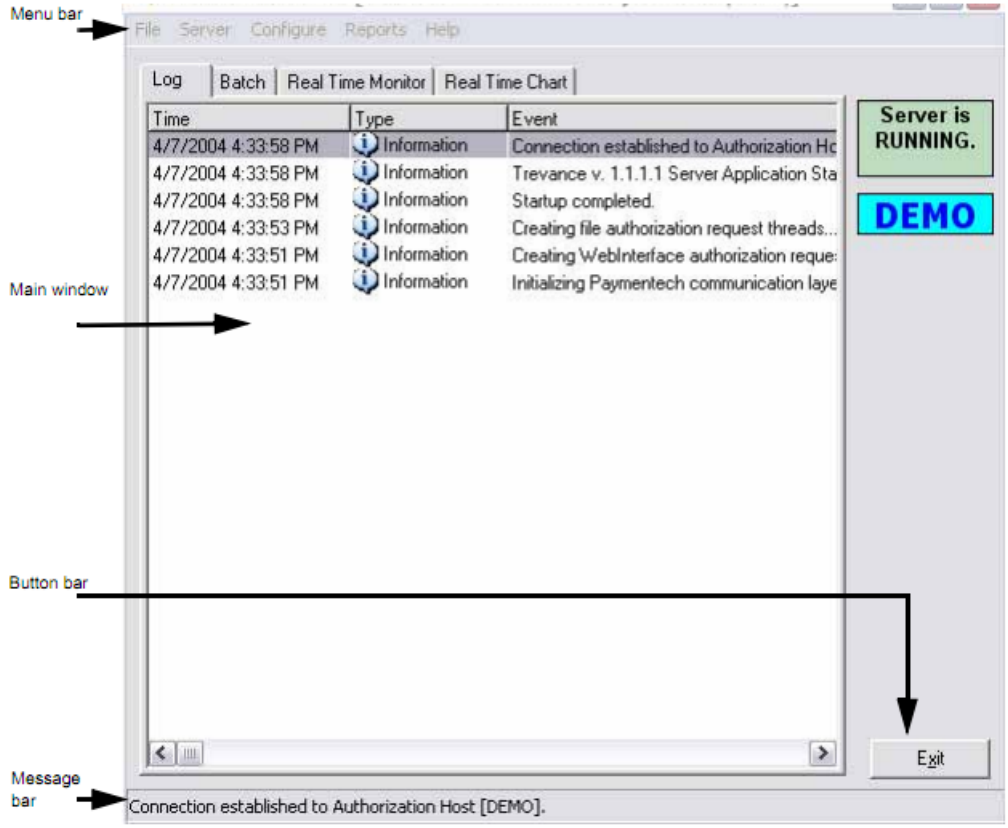
6.3.2.8 Web interface transactions

A web interface transaction is one authorization transaction from an application that is capable of sending and receiving an HTTP POST. Trevance® processes this transaction as soon as it is received (that is, in real time).

6.4 Understanding the Trevance® Screen

The main Trevance® screen contains four parts:

- Menu bar
- Main window
- Button bar
- Message bar



Some of the menus may not be available until you pause Trevance® (for example, you can't archive or configure imports until Trevance® is paused).

The following table describes the menus:

Table 6.3: Menus

Click on This Menu . . .	*To Select from These Tasks . . .*

Continued on next page

Table 6.3 – *Continued from previous page*

Click on This Menu . . .	*To Select from These Tasks . . .*
File	Print page (current screen) Export Configuration File Import Configuration File Restore from Recovery Log Archive Database Logs (archives activity log) Sweep Database (perform database maintenance tasks specific to embedded Firebird database) Verify/Repair Database (for troubleshooting only) Exit Trevance®
Server	Pause Resume Resend Batch Remove Batch (from the queue) Check Response Files Now
Configure	Set Password Users (add, delete, or change user information) Reports (change header) E-Mail Notification Scheduled Database Maintenance *Pause Server to Configure Settings Below* (pauses server) *Resume Server when Configuration Complete* (resumes server) Processor Settings Real-Time Web Interface (change settings) Batch Files (configure imports, exports, and batch file encryption) Directories (change where files are stored) Options Serial Number and Activation Key (enter or change) Set Run Mode (switches Trevance® between demo, test, and production modes) Set Server Passphrase (an encryption key to protect your data) Run Demo As (choose, for example, CN-3500 or CN-4200)
Reports	Print This Page Select Report (future)

Continued on next page

Table 6.3 – *Continued from previous page*

Click on This Menu . . .	*To Select from These Tasks . . .*
Help	User Manual (view and print) Field Reference (view and print) Get Acrobat Reader Configuration Report (build a report) Auric Systems International Home Page Maintenance Contract (available in test or production mode only) About Trevance® Transaction Gateway (find out about Trevance® , including the serial number and activation key)

6.4.0.9 About Trevance® Transaction Gateway

(find out about Trevance® , including the serial number and activation key)

There's one button on the main Trevance® screen:

Table 6.4: Menus

Click on . . .	*To . . .*
	Trevance® console (the console no longer appears on the screen, but Trevance® continues working unless you also exit the server)

7 Operation

You've configured and tested Trevance® , and you've arranged for an external application to send delimited text files to it. Now you're ready for Trevance® to automatically import, submit, and export files.

You must make sure that:

- Trevance® is in production mode.
- Trevance® is not paused.

Trevance® starts working immediately and keeps on working. You may never need to touch it again.

However, you may want to undertake some tasks in the future: pause, resume, shut down and restart the server, observe the status, delete a file, and archive log files, among others. This chapter describes those operations. It also describes how to disconnect console users.

7.1 Pausing, Resuming, Exiting, Launching the Console

7.1.1 Pausing or Resuming

You can pause from either the Server menu or the Configure menu:

- Click on Server, then Pause
- Click on Configure, then *Pause Server to Configure Items Below*.

You can resume from either the Server menu or the Configure menu:

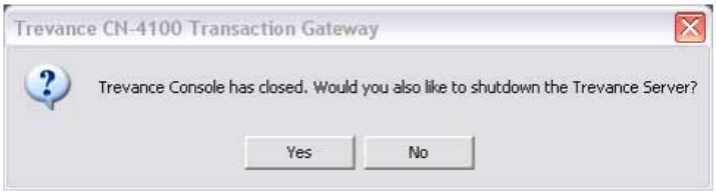
- Click on Server, then Resume
- Click on Configure, then *Resume Server when Configuration Complete*.

7.1.2 Exiting and Launching as an Application

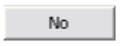
7.1.2.1 Exiting the Console without Shutting Down the Server

To exit Trevance® (close the console and hide the main screen from view):

- Click on File.
- Click on Exit to view:


Trevance CN-4100 Transaction Gateway
Trevance Console has closed. Would you also like to shutdown the Trevance Server?
Yes
No

The message appears only if you haven't exited Trevance® before and only if no other users are logged into the server.

- Click on 

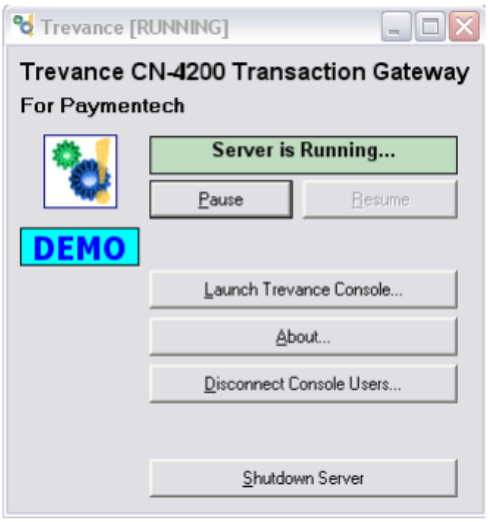
Information on shutting down the server appears later in this chapter.

7.1.3 Launching the Console from the User Interface

The user interface screen appears only when Trevance® is operating as an application (not a service).

To launch the Trevance® console (show the main screen):

1. Double click on the icon that appears on the task bar of your desktop to view:



2. Click on to view the logon screen.

3. Enter your user name and password to open the console (view the main Trevance® screen).
   If Trevance® was paused when you exited, it opens paused.
   If Trevance® was running when you exited, it opens running.

7.2 Shutting Down and Restarting the Server

The method for shutting down and restarting the server differs depending on whether Trevance® is running as an application or a service.

You should wait until there isn't any import or export activity in progress before shutting down: make sure the queue is empty, or check for response files (see page 149). After you check for response files, you can shut down; Trevance® begins processing the response file(s) when you restart the server.

Trevance® doesn't shut down immediately; it waits to finish any transactions that are in the midst of processing.

Trevance® stays paused as long as the server is shut down. But when you start up again, Trevance® *automatically begins processing transactions*, even before you open the console. This is the

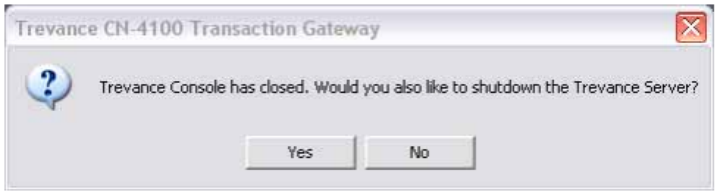
default. To configure Trevance® to restart in he paused mode, see "Changing General Options," starting on page 95.

7.2.1 When Trevance® Is an Application

7.2.1.1 Shutdown

To shut down the server:

1. Click on File.
2. Click on Exit to view:


Trevance CN-4100 Transaction Gateway
Trevance Console has closed. Would you also like to shutdown the Trevance Server?
Yes
No

   The message appears only if you haven't exited Trevance® before and only if no other users are logged into the server.

3. Click on

7.2.1.2 Restart

To restart the server:

1. Click on

2. Click on Trevance to view the logon screen.
3. Log on.

7.2.2 When Trevance® Is a Service

Shut down the service through the Windows Control Panel.

After you shut down Trevance® as a service, you can either restart it as a service or open it as an application.

Restart the service through the Windows Control Panel.

7.3 Changing the Log, Batch, and Monitor Screens

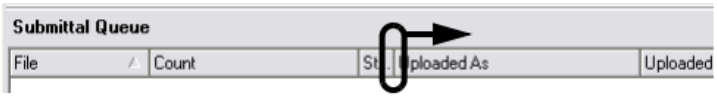
On the Log, Batch, and Monitor screens, you can change the width of columns

On the Batch and Monitor screens, you can also change the order in which information appears

This section describes how to perform those general changes.

7.3.1 Changing the Width of Columns

If the full column names aren't showing (for example, if you see St... instead of Status), click on the bar beside the column and drag it right:



7.3.2 Sorting Information

You can sort information on the Batch or Monitor screens based on any one column. For example, you can sort the Recent Batches screen by Date/Time.

1. Click on the column header.

   An arrow appears in the header to indicate whether you are sorting in ascending or descending order.

2. Click until the batches are sorted in the order you want.

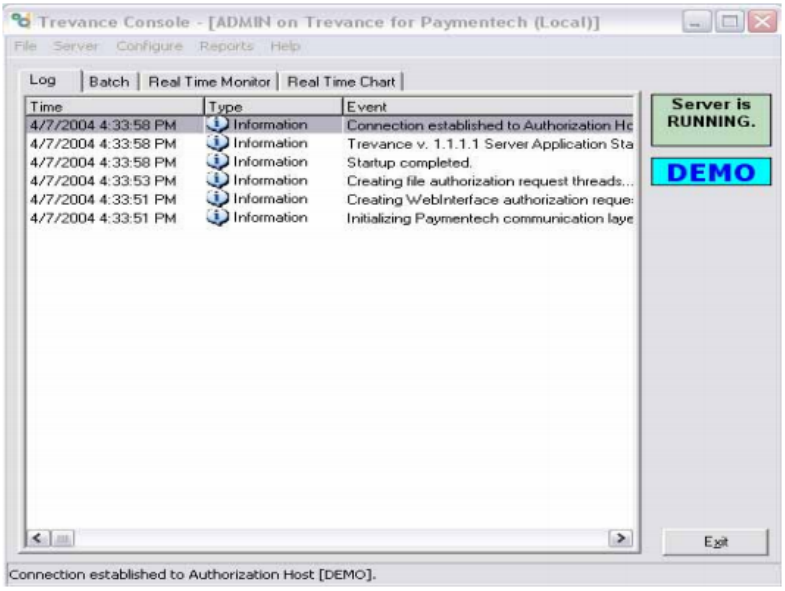
   For example, if you sort by Date/Time in descending order, you'll see the oldest batches first.

7.4 Understanding the Events Log

Trevance® logs operating events (such as pause and resume, file import and export, and submission of transactions) in two ways: on the Log screen and in a log file.

7.4.1 The Log Screen

On the Log screen, Trevance® lists the events that occur from the moment when Trevance®— starts, up to a maximum of 200 events. After 200, the oldest events disappear from the screen, although they're still available in the log file. The Log screen is reset at midnight each night or any time that you exit Trevance®.Click on the Log tab to view:


Trevance Console - [ADMIN on Trevance for Paymentech (Local)]
File Server Configure Reports Help
Log
Batch
Real Time Monitor
Real Time Chart
Time
Type
Event
4/7/2004 4:33:58 PM Information Connection established to Authorization Ho
4/7/2004 4:33:58 PM Information Trevance v. 1.1.1.1 Server Application Sta
4/7/2004 4:33:58 PM Information Startup completed.
4/7/2004 4:33:53 PM Information Creating file authorization request threads...
4/7/2004 4:33:51 PM Information Creating WebInterface authorization reque
4/7/2004 4:33:51 PM Information Initializing Paymentech communication laye
Server is RUNNING.
DEMO
Exit
Connection established to Authorization Host [DEMO].

The columns on the Log screen give you the following information:

Table 7.1: Log Screen

Column	*Information*
Time	The date (mm/dd/yy) and time (hh:mm:ss) when the event occurred

Continued on next page

Table 7.1 – *Continued from previous page*

Column	*Information*
Type	The type of event: Information (such as "submitting transaction"), Warning (such as "Rejected 20 Records") or Error (such as "error connecting to host")
Event	A detailed description of the event

7.4.2 The Log Files

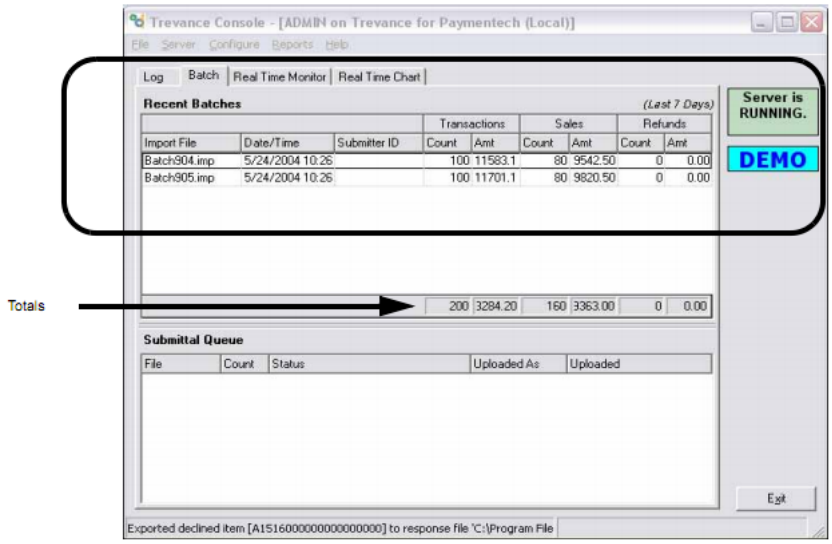
The entire log file (not just the 200 most recent events) is stored in the LOG directory and has a .LOG extension. Trevance® creates a new file beginning at midnight on every day that it runs. For example, all the operating events that occur during August 4, 2002, are logged to *trevance_20020804.log*; and all the events that occur during August 9, 2002, are logged to *trevance_20020809.log.*

You might want to remove the oldest log files periodically, to conserve space on your hard drive.

7.5 Tracking Recent Batches

Trevance® lists the batches that your processing service processed and then returned. The Recent Batches list displays information about each batch for 30 days from the date the batch was returned by the processing service. As batches leave the Submittal Queue, they automatically show up on the Recent Batches list, with two exceptions. The Recent Batches list will not record batches that failed because of improper formatting or batches that you manually removed from the queue.

1. Click on the Batch tab to view:


Trevance Console - [ADMIN on Trevance for Paymentech (Local)]
File Server Configure Reports Help
Log Batch Real Time Monitor Real Time Chart
Recent Batches
(Last 7 Days)
Server is RUNNING.
DEMO
Import File Date/Time Submitter ID Transactions Count Amt Sales Count Amt Refunds Count Amt
Batch904.imp 5/24/2004 10:26 100 11583.1 80 9542.50 0 0.00
Batch905.imp 5/24/2004 10:26 100 11701.1 80 9820.50 0 0.00
Totals
200 3284.20 160 3363.00 0 0.00
Submittal Queue
File Count Status Uploaded As Uploaded
Exit
Exported declined item [A1516000000000000000] to response file 'C:\Program File

The Recent Batches window shows the following information:

Table 7.2: Recent Batches Window

Column	*Information*
Import File	The name of the batch file that Trevance® imported
Date/Time	The date and time when the submission was completed (that is, when the processing service returned the batch)
Submitter ID	The submitter ID for the batch (set up when you configured processor settings)
Transactions	The total number (Count) and amount (Amt) of transactions in the batch
Sales	The total number (Count) and amount (Amt) of sales transactions in the batch

Continued on next page

Table 7.2 – *Continued from previous page*

Column	*Information*
Refunds	The total number (Count) and amount (Amt) of refund transactions in the batch

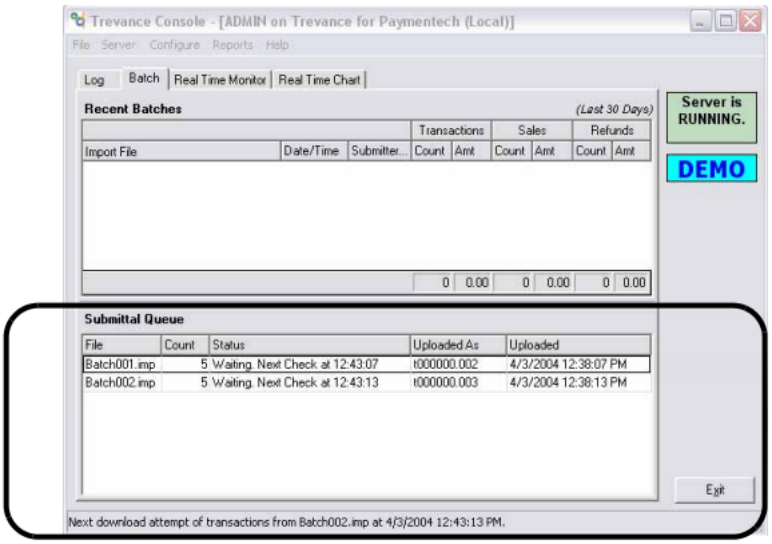
7.6 Using the Batch Submittal Queue

Trevance® has a queue that shows the point where each batch transaction is in the submittal process. The Submittal Queue lists imported batch files currently in the Trevance® system. The queue describes each imported file and tells you its status (for example, importing, uploading, waiting, downloading, or exporting). When Trevance® has exported all the transactions in the file to your external application, the file disappears from the queue. (When the file returns from the processing service, it automatically shows up on the Recent Batches list.)

From the queue, you can check response files, remove a batch, resend a batch, and check response files. These procedures should be used with care, especially removing and resending a batch.

7.6.1 Viewing the Submittal Queue

Click on the Batch tab to view:


Trevance Console - [ADMIN on Trevance for Paymentech (Local)]
File Server Configure Reports Help
Log Batch Real Time Monitor Real Time Chart
Recent Batches
(Last 30 Days)
Server is RUNNING.
DEMO
Import File Date/Time Submitter... Transactions Count Amt Sales Count Amt Refunds Count Amt
0 0.00 0 0.00 0 0.00
Submittal Queue
File Count Status Uploaded As Uploaded
Batch001.imp 5 Waiting. Next Check at 12:43:07 t000000.002 4/3/2004 12:38:07 PM
Batch002.imp 5 Waiting. Next Check at 12:43:13 t000000.003 4/3/2004 12:38:13 PM
Exit
Next download attempt of transactions from Batch002.imp at 4/3/2004 12:43:13 PM.

The columns on the Submittall Queue screen give you the following information:

Table 7.3: Submittal Queue

Column	*Information*
File	The name of the imported file in the queue

Continued on next page

Table 7.3 – *Continued from previous page*

Column	*Information*
Status	Whether the transactions in the file: • Are being imported (Importing; Imported) • Are being uploaded (Uploading; Uploaded) • Are waiting the five-minute delay between the time Trevance® uploads and the time it checks for downloads; the time of the next check is given (Waiting. Next check at ...) • Are being downloaded (Downloading; Downloaded) • Are being exported (Exporting; Exported)
Upload As	The name of the file that your processing service recognizes; Trevance® automatically assigns this name
Uploaded	The date and time when Trevance® sent the file to your processing service

Several additional status messages may also appear on your screen. For example, if Trevance® is paused while transactions are being processed, you might see these messages: Ready to Format for Upload, Ready to Upload, Waiting (Paused), Ready to Download, or Ready to Export. Also if the processing fails for any reason (for example, because of a power failure), you might see: Partial Import (Failed).

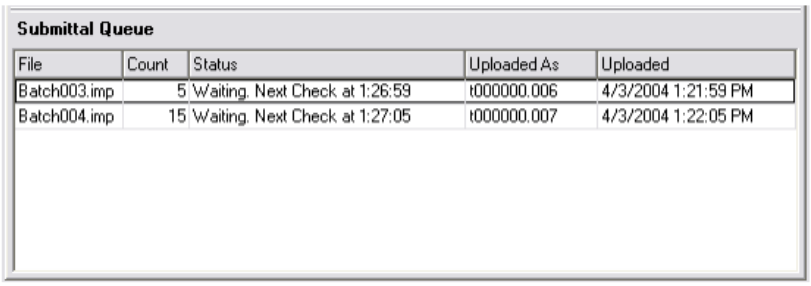
7.6.2 Removing a Batch

Trevance® allows you to remove any batch from the submittal queue. Auric Systems International *does not recommend this procedure.*

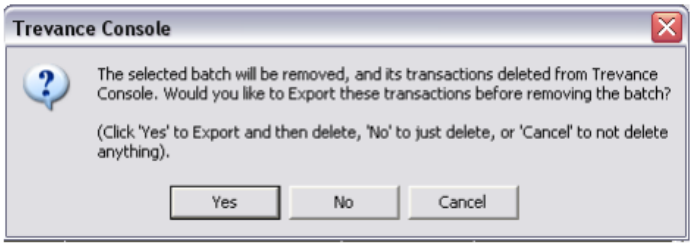
If you remove a batch from the queue, it won't show up on the Recent Batches list, because it was never submitted.

To remove a batch from the queue:

1. Click on Server.
2. If Trevance® is not paused, click on Pause.
3. Click on the Batch tab to view the files in the Submittal Queue:



4. Click on the file you want to remove (in this case Batch004.imp).
5. Click on Server.
6. Click on Remove Batch to view:


Trevance Console
The selected batch will be removed, and its transactions deleted from Trevance Console. Would you like to Export these transactions before removing the batch?
(Click 'Yes' to Export and then delete, 'No' to just delete, or 'Cancel' to not delete anything).
Yes
No
Cancel

You have three choices:

- Click on, Yes then click on OK and the transactions are immediately and automatically exported. Then the file is immediately deleted. You should *always* export if you are using Trevance® in the production mode.
- Click on No and the file is immediately and automatically deleted. Nothing is exported.

- Click on Cancel and nothing happens. (Once you resume, Trevance® exports the file normally.)
- Click on Server.
- Click on Resume.

7.6.3 Resending a Batch

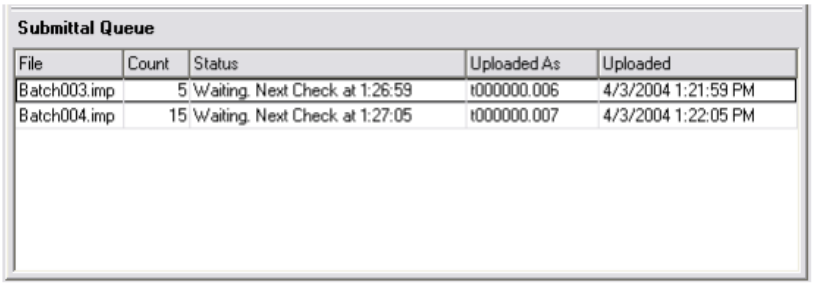
Occasionally, your processing service may ask you to resend a batch.

You should resend a batch only if your processing service or Auric Systems International asks you to.

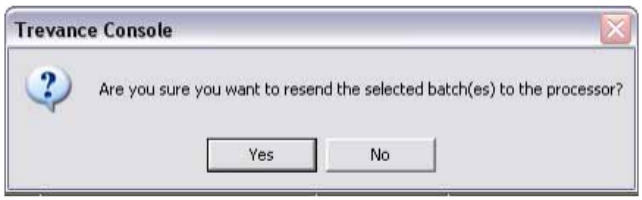
You *must contact your processing service before you resend a batch.*

To resend a batch:

1. Click on Server.
2. If Trevance® is not paused, click on Pause.
3. Click on the Batch tab to view the files in the Submittal Queue:



4. Click on the file you want to resend (in this case, Batch004.imp).
5. Click on Server.
6. Click on Resend Batch to view:



7. Click on Yes to view a message like the following:

8. Click on Server.
9. Click on Resume.
10. The file is resent to the processing service.

7.6.4 Checking Response Files

Trevance® automatically checks for response files at set intervals. If you prefer, you can request an immediate check for any files waiting for retrieval.

To check response files, Trevance® must be working. If it is paused, this selection is not available.

- Click on Server.
- If Trevance® is paused, click on Resume.
- Click on Check Response Files Now.

If Trevance® finds any file waiting for retrieval, it retrieves the file. A message appears at the bottom of your screen to let you know if any files were found.

7.7 Using the Real-Time Monitor and Chart

The Real Time Monitor provides a summary of real-time web interface transactions processed since midnight. (It's reset at the end of the day; that is, at midnight.) It shows the total number and dollar value of each type of transaction. It updates every ten

seconds. The Real Time Chart shows the same information in chart form.

Transactions that have been archived are not included in the Real Time Monitor and Real Time Chart.

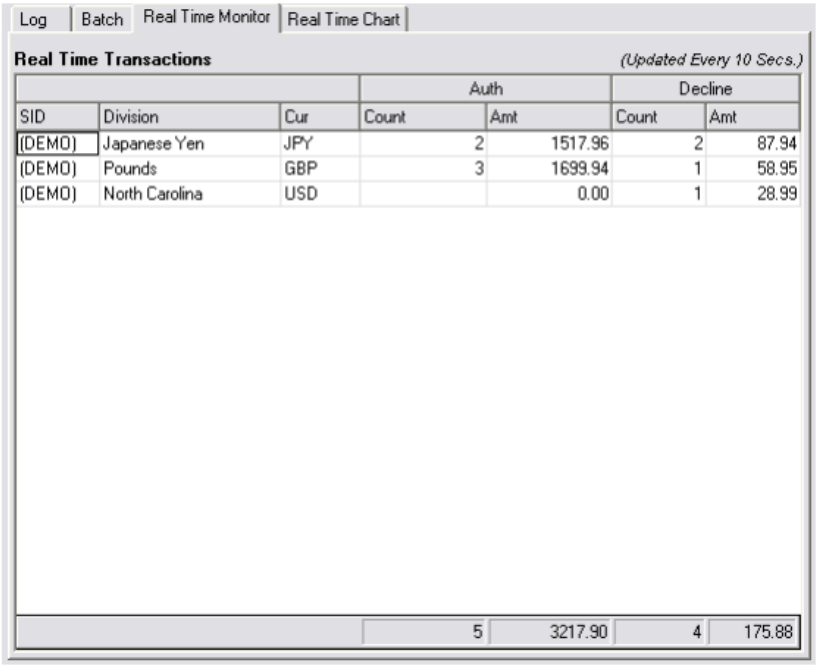
7.7.1 Viewing the Real-Time Monitor

The Real Time Monitor lists the processed authorization transactions handled by Trevance® in real-time. It calculates the total number and total value of each type of transaction that Trevance® handled.

If you have multiple submitter and division IDs, Trevance® totals the transactions by submitter ID and division ID. The value is given in the currency associated with the specific division ID.

The monitor may track transactions by several categories that depend on your processing service and on how you configured your processor settings.

To view the monitor, click on the Real Time Monitor tab.



The columns on the Real Time Monitor screen give you the following information:

Table 7.4: Real Time Monitor

Column	*Information (from the day you choose until today)*
SID	Submitter ID
Division	Division ID or description (depending on how you configured processor settings)
Cur	Currency (the default currency is U.S. dollars)
Auths	The total number (Total Count) and value (Amt) of authorizations
Declines or Captures or Refunds	The total number (Total Count) and value (Amt) of the indicated transactions

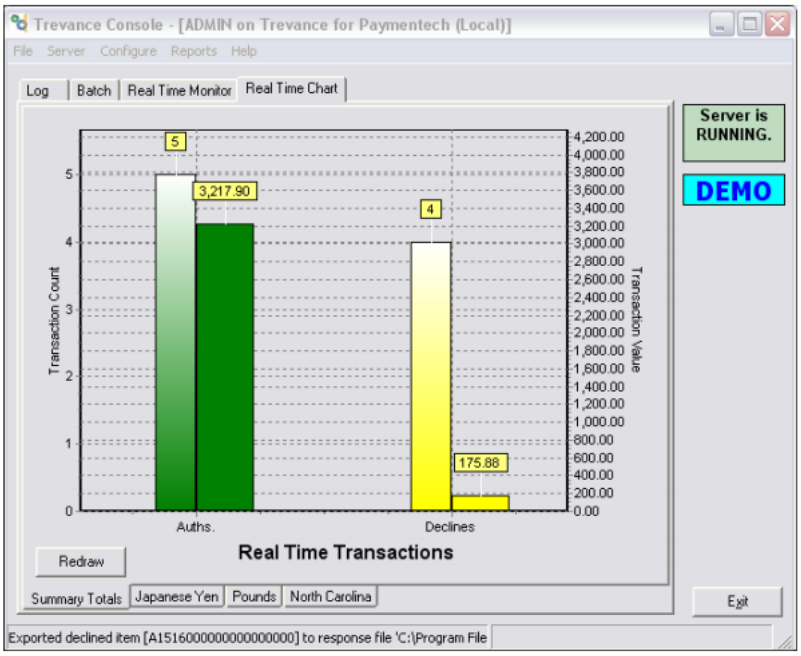
The default currency is U.S. dollars.

The previous screen shows transactions that were processed in multiple currencies (for example, Japanese yen and British pounds) and from a division in North Carolina. In the SID, Division, and Cur (currency) columns, Trevance® places the information provided when you configured processor settings (see "Part II. Your Processing Service," starting on page 193.

7.7.2 Viewing the Real-Time Chart

The Real Time Chart shows the same transaction information as the monitor, but in the form of a bar graph.

To view the chart, click on the Real Time Chart tab.



Each type of transaction has its own two-part bar. The left part shows the total transaction count (for example, 5 authorizations); the right part shows the total transaction value (for example, $3,217.90).

If you are using multiple currencies (for example, dollars and Japanese yen), the summary totals won't make sense. To see the results for each currency, click on the appropriate tab.

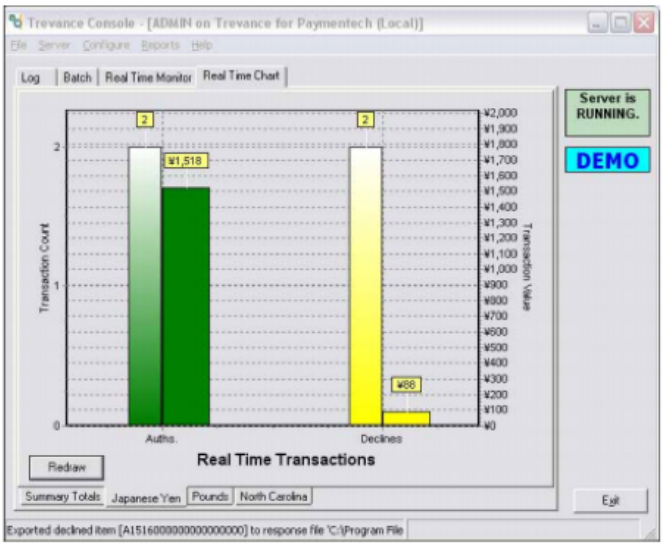
The label on the tab shows either the division ID or the division description, depending on how you configured processor settings.

You can change your view of the chart.

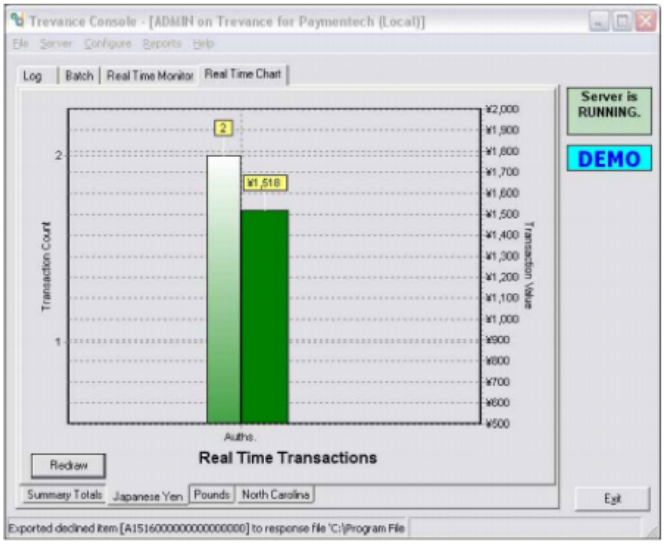
7.7.3 Changing the Real-Time Chart

To focus in on part of the chart, left click and drag your mouse to the right. To change the image, left click again and drag your mouse either left or right. To restore the chart its original appearance, click on

Compare the following Real Time Chart screens.



The graph above hasn't been moved.



Here's the same graph, after a drag right. (Note the change in scale for the Transaction Count and Transaction Value columns.)

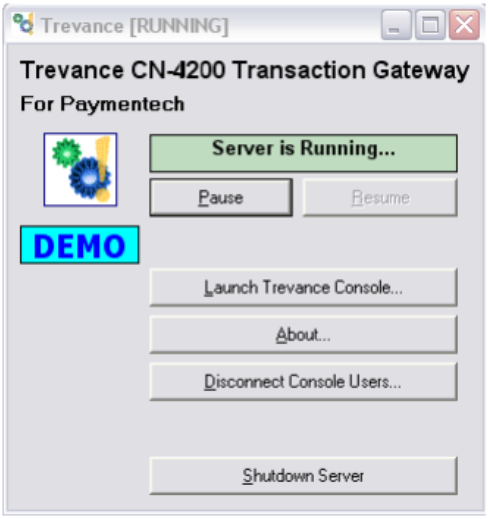
7.8 Disconnecting Console Users

You may want to disconnect console users if you logged into a remote machine as an administrator (for example) and now want

to log into a local machine. (The administrator is allowed to log in only once.)

7.8.1 Disconnecting Users When Trevance® Runs As an Application

1. Double click on the icon that appears on the task bar of your desktop to view a screen like the following:



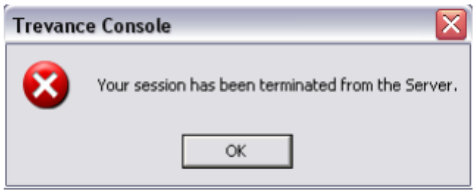
2. Make sure the server is paused. If necessary, click on

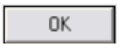
3. Click on

to view:

4. Click on

to view:



5. Click on 

   You have now terminated all users from the server.

7.8.2 Disconnecting Users When Trevance® Runs As a Service

You must shut down the server from the control panel to automatically disconnect all users from the server.

8 Maintenance

This chapter describes how to maintain and troubleshoot Trevance®

You'll also want to check out the information in Chapter 4 on configuration reports (see page 103) and debug logs (see page 101).

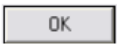
8.1 Maintenance Contract

Trevance® comes with a year of free maintenance, support, and updates. When the year expires, you may renew the maintenance contract by contacting Auric Systems International.

Maintenance information appears on the Help menu *after* you've entered a valid serial number and activation key.

For information on the expiration date of your contract and on renewing the maintenance contract:

1. Click on Help.
2. Click on About Trevance® Transaction Gateway.
3. Scroll down to MaintenanceExpires to find the expiration date for your maintenance contract.

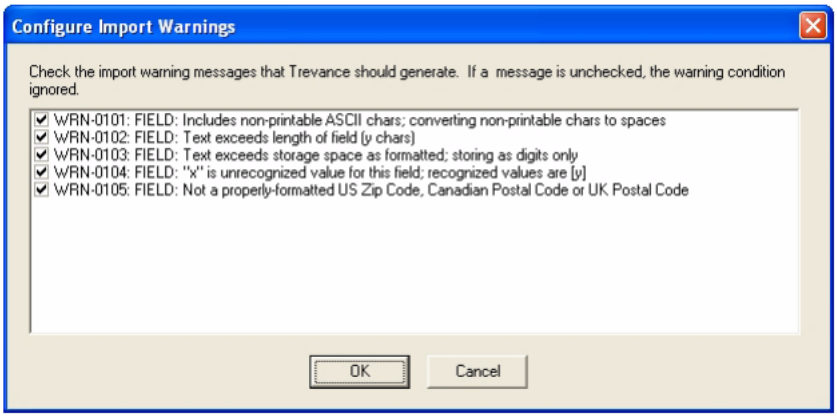
   You must renew your maintenance contract on or before the expiration date shown.
4. Click on 

5. Click on Server.
6. Click on Pause.
7. Click on Help.
8. Click on Maintenance Contract to view a screen like the following:

Renew Maintenance Contract
To renew your maintenance contract, follow these easy steps:
1.
Follow this link to Auric Systems International's support page to obtain a new activation key:
http://www.AuricSystems.com/renew_4200
2.
Copy and paste or type in the new activation key, click OK and you're ready to go!
Activation Key:
Cancel
OK

9. Follow the directions for renewing your maintenance contract or call Auric Systems International.

8.2 Configure Warnings


Configure Import Warnings
Check the import warning messages that Trevance should generate. If a message is unchecked, the warning condition ignored.
WRN-0101: FIELD: Includes non-printable ASCII chars; converting non-printable chars to spaces
WRN-0102: FIELD: Text exceeds length of field (y chars)
WRN-0103: FIELD: Text exceeds storage space as formatted; storing as digits only
WRN-0104: FIELD: "x" is unrecognized value for this field; recognized values are [y]
WRN-0105: FIELD: Not a properly-formatted US Zip Code, Canadian Postal Code or UK Postal Code
OK
Cancel

Trevance® generates a number of import warnings that can be useful during initial development and testing, but less useful during live production runs.

For example, Trevance® checks for validly formatted ZIP or Postal Codes. These warnings are useful during development in ensuring the proper information is being sent to Trevance® . However, in production environments where you are dealing with real-life data which might be mis-entered, having Trevance® generate these errors is not as helpful, clutters up the log file, and makes it difficult to locate other, useful warnings and errors.

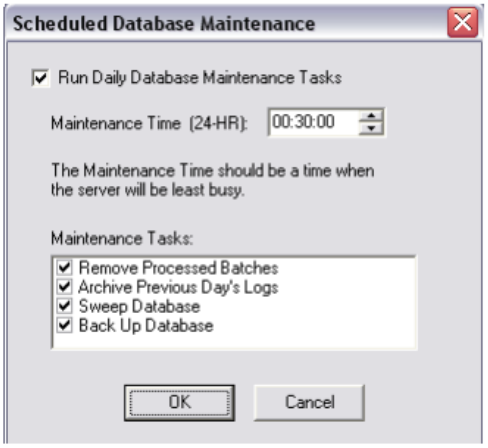
Warnings are disabled by selecting the Warning... entry in the Configure menu. Each of the import warnings in the Configure/Warnings dialog may be disabled by unchecking the associated checkbox and clicking OK.

8.3 Scheduling Database Maintenance

You may maintain the database either automatically or manually (as described later in this chapter). Auric Systems International recommends automatic maintenance.

To automatically maintain the database:

1. Click on Configure.
2. Click on Scheduled Database Maintenance to view:



   The default is a complete scheduled maintenance of the database, beginning at half past midnight (00:30:00) daily.

   If you click on Run Daily Database Maintenance Tasks to remove the check-mark, none of the daily maintenance tasks runs automatically. Auric Systems International recommends that you do *not* remove the check-mark.

3. Change the time for performing maintenance tasks. The default is half-past midnight (00:30:00). Select a time so that maintenance occurs at these times:

- When the server is the least busy. Trevance® continues to process transactions while the maintenance tasks are being run.
- After all scheduled e-mail notifications are sent out and you've created all the reports you want. Otherwise, you won't be able to create reports because the daily maintenance tasks will have already removed and archived the data. For information on scheduling e-mail notifications, see "Configuring and Sending E-Mail Notifications (Messages)" on page 180.
- Before 1 a.m. or after 3 a.m. If you schedule database maintenance tasks between 1:00 a.m. and 3:00 a.m., you'll run into problems when the time changes between standard and daylight savings time. (In spring, clocks jump from 1:59 a.m. to 3:00 a.m.; in fall, clocks jump from 1:59 a.m. to 1:00 a.m.)

4. Make sure there's a check-mark next to any maintenance tasks you want to run at the time you selected:

Table 8.1: Scheduling Database Maintenance

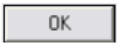
Task	*Definition*
Remove Processed Batches	Deletes batches that have been processed and exported. To reduce the processing load during high-traffic times, Trevance® waits to delete batches. Make sure you run this maintenance task nightly to keep the database from growing too large.

Continued on next page

Table 8.1 – *Continued from previous page*

Task	*Definition*
Archive Previous Day's Logs	Archives the previous day's transaction activity logs; the batch and real time files are archived separately. Make sure you run this maintenance task nightly to keep the database from growing too large. If for some reason the activity log archive hasn't run for a few days, the automated process also archives transaction activity older than the previous day.
Sweep Database	Performs a number of database maintenance tasks specific to the embedded Firebird database.
Back Up Database	Copies the database to the directory you select, while Trevance® is running.

If you want to change the default archive or backup directory, see "Configuring Directories" on page 91.

5. Click on 

8.4 Backing Up and Restoring the Database Manually

You should back up the Trevance® database regularly. You may back up either automatically (as described previously) or manually.

Auric Systems International recommends that you schedule a nightly automatic backup of the database as described on page 161. If you are running debit cards, you should also back up the recovery log directory nightly.

To manually back up:

1. Click on Server.
2. Click on Pause.
3. Using Windows Explorer, look under Program Files to find the Trevance® directory.
4. Open the Trevance® directory to find the Data directory.
5. Copy the Data directory from your hard drive on to a zip disk or floppy.

If you need to restore the database, first pause and exit Trevance®. Then copy the backed up files over the existing files in the Trevance® directory.

8.5 Deleting Old Files

You can delete old files from any directory; however, deleting old files affects Trevance® 's file naming.

Trevance® always names files using the lowest available number. For examples:

- ABC.DNE
- ABC_001.DNE
- ABC_002.DNE
- ABC_003.DNE
- ABC_004.DNE

In this example, the next .DNE file that Trevance® creates is named ABC_005.DNE.

But suppose, before that happens, you delete the old files ABC_001.DNE and ABC_002.DNE. In that case, the next .DNE file that Trevance® creates is named ABC_001.DNE.

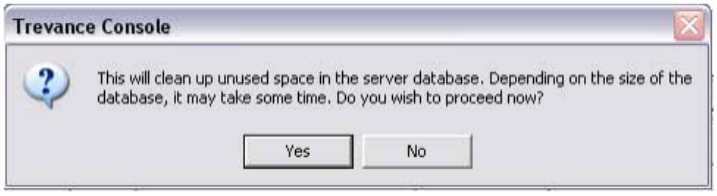
Therefore, the number 001 doesn't guarantee that ABC_001.DNE is your oldest file. To prevent problems, make sure each file has a unique name and check the date of a file before deleting.

8.6 Sweeping the Database Manually

The sweep operation performs a number of database maintenance tasks specific to the embedded Firebird database. Auric Systems International recommends a nightly automatic sweep as described on page 161. However, if you shut down and start up frequently and if you see a drop in performance, you might try a manual sweep.

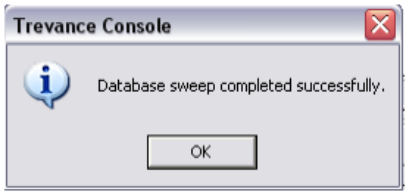
To sweep the database:

1. Click on Server.
2. Click on Pause.Click on File.
3. Click on Sweep Database to view:


Trevance Console
This will clean up unused space in the server database. Depending on the size of the database, it may take some time. Do you wish to proceed now?
Yes
No

4. Click on

   The sweep continues until the following message appears:

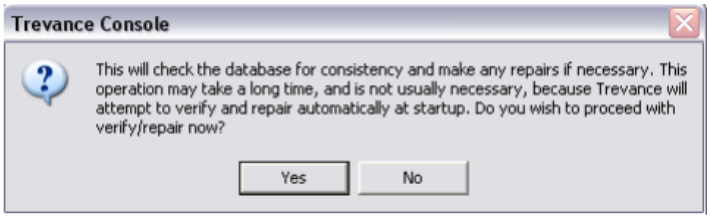


5. Click on

8.7 Verify/Repair

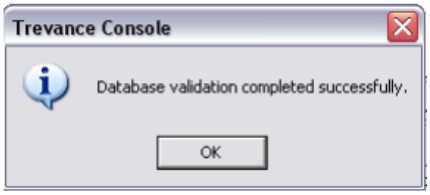
You can ask Trevance® to check the database for consistency and make any necessary repairs. Because Trevance® always attempts to recover automatically at startup, you should verify/repair only if asked to do so by your technical support or by Auric Systems International.

1. Click on Server.
2. Click on Pause.Click on File.
3. Click on Verify/Repair Database to view:


Trevance Console
This will check the database for consistency and make any repairs if necessary. This operation may take a long time, and is not usually necessary, because Trevance will attempt to verify and repair automatically at startup. Do you wish to proceed with verify/repair now?
Yes
No

4. Click on

   The verify/repair operation continues until the following message appears:



5. Click on

8.8 Archiving

Trevance® maintains an activity log that tracks:

- Processed web interface transactions
- Processed batch transactions
- Batch summaries

You should set up the activity log to archive automatically as explained in "Scheduling Database Maintenance" on page 161 (Archive Previous Day's Logs).

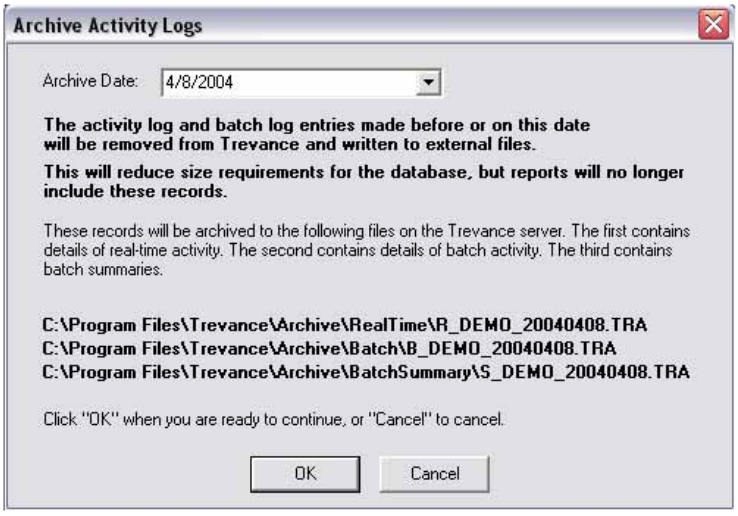
The activity log is exported to a delimited text file with a .TRA extension in the ARCHIVE directory. Archiving creates one file for batch transactions, another file for batch summaries, and a third file for web interface transactions. After archiving:

- The file for batch transactions appears in the BATCH subdirectory of the ARCHIVE directory.
- The file for batch summaries appears in the BATCHSUMMARY subdirectory of the ARCHIVE directory.
- The file for web interface transactions appears in the REALTIME subdirectory of the ARCHIVE directory.

These files can be imported into a spreadsheet or database for reporting or analysis.

Under some circumstances, you may also want to archive manually:

1. Click on Configure.
2. Click on *Pause Server to Configure Items Below*.
3. Click on File.
4. Click on Archive Database Logs to view:


Archive Activity Logs
Archive Date:
4/8/2004
The activity log and batch log entries made before or on this date will be removed from Trevance and written to external files.
This will reduce size requirements for the database, but reports will no longer include these records.
These records will be archived to the following files on the Trevance server. The first contains details of real-time activity. The second contains details of batch activity. The third contains batch summaries.
C:\Program Files\Trevance\Archive\RealTime\R_DEMO_20040408.TRA
C:\Program Files\Trevance\Archive\Batch\B_DEMO_20040408.TRA
C:\Program Files\Trevance\Archive\BatchSummary\S_DEMO_20040408.TRA
Click "OK" when you are ready to continue, or "Cancel" to cancel.
OK
Cancel

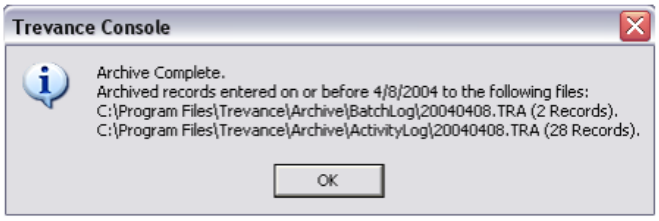
Trevance® automatically creates a name for each archive file, based on the Archive Date.

For example, R_20040408.TRA contains real-time transactions completed on or before 2004, in April (04), and on the 8th day.

5. Select a cutoff date (Archive Date) for the processed transactions that will be archived. Do one of the following:

- Type a date in the Archive Date box (including the slashes).
- Or click on to view a calendar and select a date.
- Or keep the default date, which is 30 days earlier than today's date. (For example, if today is August 10, the default date is July 11.)

6. Click on OK to start the archive.
7. Wait. After a while, you'll see a message like the following:


Trevance Console
Archive Complete.
Archived records entered on or before 4/8/2004 to the following files:
C:\Program Files\Trevance\Archive\BatchLog\20040408.TRA (2 Records).
C:\Program Files\Trevance\Archive\ActivityLog\20040408.TRA (28 Records).
OK

8. Click on OK
9. Trevance® archived all transactions processed on or before the date you chose.

9 PaymentVault™

All versions of Trevance® now support PaymentVault™ technology.

PaymentVault technology consists of two components:

- Unique Tracking ID (UTID) generation and short-term UTID storage in Trevance®.
- external PaymentVault server for long-term UTID storage.

The goal of the PaymentVault technology is to reduce the number of times your applications need to 'touch' a credit card number.

With PaymentVault, the payment processing work flow is as follows:

- merchant accepts credit card on secured web site.
- credit card sent to Trevance® through real-time interface for Authorization.
- if Authorization is successful at payment processor, Trevance® converts the account number into a Unique Tracking ID (UTID) and returns that value to the merchant.
- Trevance® stores the UTID and the AES-encrypted account number for later retrieval.
- at deposit/capture time, the merchant sends the UTID instead of the account number.
- Trevance® looks up the account number from the UTID and sends the account number to the Payment Processor.

This approach is independent of the Payment Processor.

9.1 PaymentVault Server

The UTID and account information is stored in Trevance® for later retrieval. This works well if you only need to keep the account information around for a few hours, or a few days, until you send your deposit transaction.

However, this approach is not recommended if you intend to keep your account numbers around for a few weeks (or even months or years in a recurring billing situation).

Auric Systems created the PaymentVault Server for long-term storage. The PaymentVault server integrates with Trevance® (and CN!Express) to provide long-term storage for account information.

The PaymentVault server is currently available as a customizable solution based on your specific needs. Particular customizations Auric can provide are:

- account aging (when to remove UTIDs from long-term storage)
- tracking recurring billing steps
- various back-end databases for UTID/account storage
- direct integration with merchant systems
- merchant-specific custom interfaces and features

The PaymentVault technology built into Trevance® is totally optional.

The PaymentVault Server is a customized add-on for use with Trevance® and CN!Express payment processing applications. Please contact Auric Systems International for more information on the PaymentVault Server.

The combination of Trevance® and PaymentVault have undergone third-party PABP assessment. Please view Visa's PABP list of validated payment applications for PABP status:

http://www.usa.visa.com/merchants/risk_management/cisp_payment_applications.html

9.2 UTID Storage

Trevance® not PaymentVault, generates the UTID value and encrypts the account number. PaymentVault is strictly a storage facility. It does not have the ability to unencrypt data. UTIDs stored in PaymentVault are not only separated from the Personally Identifiable Information (card holder name, card expiration date, etc.) but are also separated from the encrypt/decryption keys.

Trevance® provides short-term storage for UTID values. Trevance® can hold UTIDs for a user-defined number of days up to 30. An

optimal Trevance® storage time is a day or two longer than the length of time you typically take to do the initial deposit after an intial auth. This saves the PaymentVault look-up time when performing the deposit since it is still stored in Trevance®.

Trevance® transfers batches of new UTID values to PaymentVault every minute. These UTID values remain in Trevance® and there is now a copy of them in PaymentVault. Trevance® also has the ability to move the UTIDs immediately, in real-time.

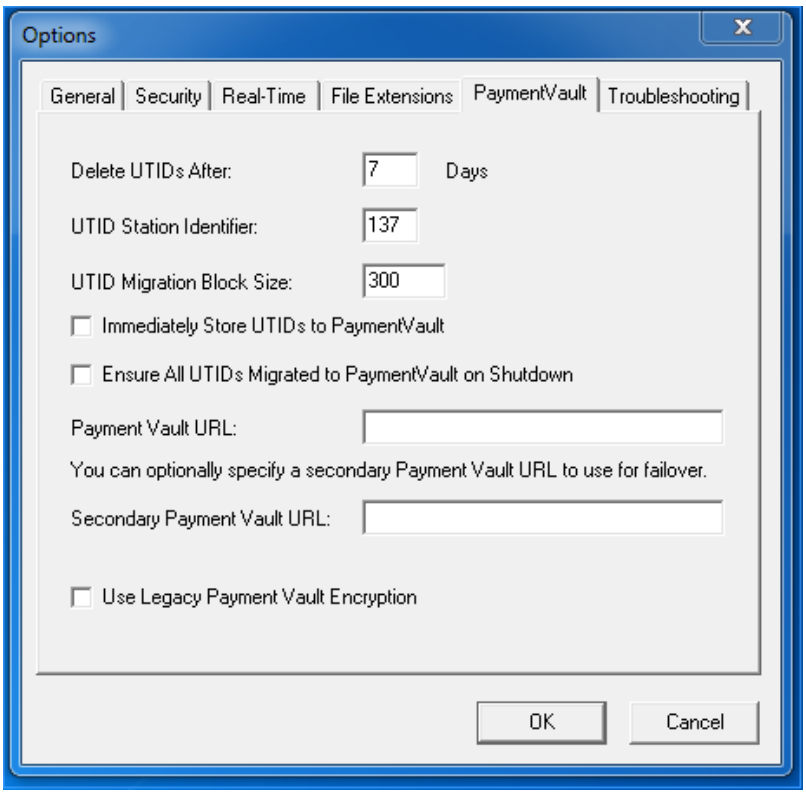
When Trevance® receives a UTID request, it first looks to see if it has that value locally. If it does not, it requests the data associated with that UTID from PaymentVault and then decrypts it.

9.3 Configuring PaymentVault

The PaymentVault settings allow you to set up PaymentVault UTID support and connect to an optional external PaymentVault Server.

To configure PaymentVault settings:

- Click on Configure.
- Click on Options.
- Select the PaymentVault tab to view:



Delete UTIDS After: Trevance® deletes UTIDs this many days after they are stored in Trevance® . This number should be kept fairly low in order to not clutter up your local Trevance® database with UTID information. The intent is to keep UTIDs you may need in the near future locally in Trevance® and store UTIDs you need long term in the PaymentVault Server. Deleting UTIDs from Trevance® does not delete them from the PaymentVault server.

UTID Station Identifier: The PaymentVault technology is typically configured so that the application (such as Trevance®) generates the UTID and PaymentVault stores it. This approach is taken to ensure we can generate a high-speed stream of UTIDs. Trevance® CN-4250 needs to generate UTIDs at up to 30 transactions per second on the real-time interface, and generates them even more rapidly when processing batch transactions. These high speeds are difficult to maintain if each and every transactions went

through a remote web interface.

Although the possibility of a collision between two UTIDs is extremely low, Trevance® adds a UTID Station Identifier to each UTID value. This has two purposes:

- reduce even further the possibility of a collision between UTID values generated by two copies of Trevance®
- be able to track which copy of Trevance® generated the UTID.

When Trevance® starts, the UTID Station Identifier defaults to the digits of the last octet of your local IP address. If the IP address of the machine on which Trevance® is installed is 10.25.18.187, then the UTID Station Identifier is 187. This may be manually changed.

You must carefully check these values if you happen to be running two copies of Trevance® (or CN!Express) on two different subnets, or if you move Trevance® from one machine to another.

Changing this value has no effect on how UTID values are looked up. This only alters how they are generated.

PaymentVault Server: If you are using the optional PaymentVault Server, enter the URL for accessing that server in this field. Otherwise leave blank. See PaymentVault documentation for details.

UTID Migration Block Size: The number of UTIDs sent to PaymentVault in a group

Immediately Store UTIDs to PaymentVault: Configures PaymentVault to add a UTID immediately, for each transaction. See PaymentVault documentation for details.

Legacy PaymentVault Encrpytion: Encryption using local keys rather than managed keys. Only for use in specific scenarios.

9.4 Returning UTIDs from Trevance®

PaymentVault UTID values are generated whenever you configure Trevance® to export a UTID.

UTID values must be presented to Trevance® in the UTID field, not the Account field (where you would pass a credit card account number).

A typical UTID from Version 3 is 39 ASCII characters and looks something like this:

S1hVTm1gHKxFu2ybwdeim17DXYcAAAcB1400822

The last four digits are the cardholder account. The three characters before that are the station identifier.

Previous UTID's, from older versions of Trevance® have 52 ASCII characters, including the hyphen, and look something like this:

4xV9JySYJaZPG8t3O-3DCIiS4qC3siP7 -hRjiAGgl4AAAPS-187

The last three characters are the station identifier.

9.5 Batch Tokenize-Only

Because UTID transactions do not go to the back-end payment processor, all UTID transaction types may only be imported through a special UTID-specific file format. *UTID actions are not supported and may not be supplied in standard transaction import (.IMP) files.*

There are two specific file formats for UTID operations, one for import, and one for export. The import file is expected to have the extension .TOKEN, while the export file will have the extension .UTID. This is to distinguish these files from standard import and export files.

The TOKEN and UTID files, unlike the configurable .IMP and .EXP transaction files, include a fixed set of fields:

.TOKEN Fields

MRCHORDR :	An identifier, used to match up the response with the .UTID file.

ACTION :	The action, one of U, UD, UC
ACCT:	The account number to tokenize. Send for U action only.
UTID:	The UTID to delete or check. Send for UD and UC actions only.

*Does not have to reference a real order number.

MRCHORDR field can be used to track the submitted cardholder account with the exported UTID. Trevance® does not export the account number during batch tokenization.

ACTIONS:

- Enter "U" to generate a UTID
- Enter "UC" to check that the supplied UTID is valid, . This will return valid if the UTID is stored locally on the Trevance® server or in a configured Payment Vault.
- Enter "UD" To delete a UTID. This action deletes the UTID from local storage and from Payment Vault, if Payment Vault is configured.

Once the import file has been saved as .TOKEN, simply resume the server. No further configuration is necessary. You will then receive a .UTID file, in your export folder, which contains the following fields:

.UTID Fields

MRCHORDR :	An identifier, used to match up the response with the .UTID file.*
ACTION :	Echoed action from the .TOKEN file
ACCT:	The last 4 digits of the tokenized account number on successful lookup
UTID:	The generated UTID for action U

LAS:	Last action succeeded. Y or N
ASIRESP:	Response code (see below)
RESPTEXT:	Text description of the response code in ASIRESP

These values may be returned for the ASIRESP field in the UTID response file:

UTID File Responses

100:	Approved
309:	Local Reject Lookup UTID Failed
310:	Local Reject Record UTID Failed
901:	Failed UTID lookup

9.6 Real-Time Use of Tokenization

To look up a UTID, or to check that the supplied UTID is valid:

- Enter "UC" in the ACTION field.
- Enter the UTID in the UTID field

Returns:

- LAS = Y on successful lookup, N on failed lookup.
- ACCT = last 4 digits of tokenized account number if successful

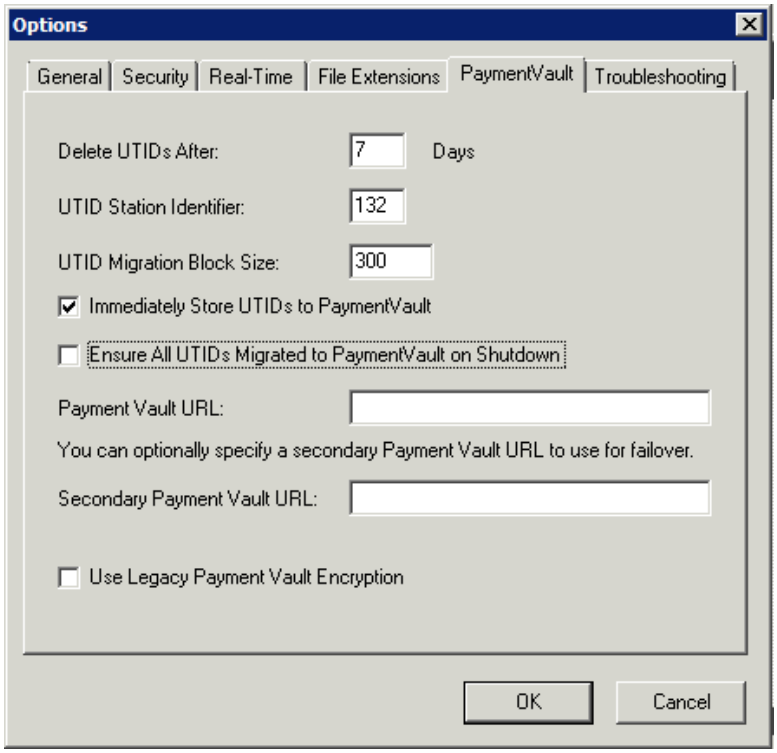
To delete a UTID from local storage and from PaymentVault, if PaymentVault is configured, enter "UD" in the ACTION field.

Returns:

- LAS = Y on success, or N if the UTID was not found.

You will see "UTID Delete succeeded" in the comment section. Click OK after entering Payment Vault URL

9.7 Real-Time UTID Updates



Trevance® transfers batches of new UTID values to PaymentVault™ every minute. In order to transfer UTIDs to PaymentVault™ immediately, this option needs to be configured in the Console.

- From the Trevance® Console, select PaymentVault from the Options tab
- Select the option to "Immediately Store UTIDs to PaymentVault"
- Enter the PaymentVault URL

- Click OK
- Trevance® is now configured to add a UTID to PaymentVault immediately, for each transaction

10 Reports and Emails

hiii

This chapter describes how to configure, print, and save information on the screen in the form of a report. It also describes how to create and send hourly, batch, daily, and special messages to your e-mail concerning system events (for example, who logged in and when).

For information on configuration reports, see “Producing a Configuration Report” on page in section 3.9

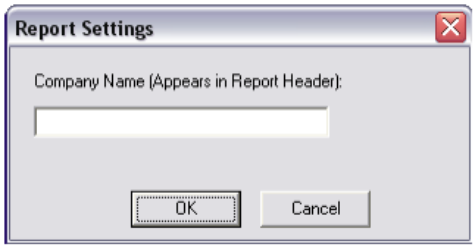
10.1 Configuring, Printing, and Saving Reports

You can print the information from any screen as a report.You can configure the report by specifying the information you want in the report heading.

10.1.1 Configuring Reports

To indicate the company name that appears in the heading of any report:

1. Click on Configure.
2. Click on Reports to view:



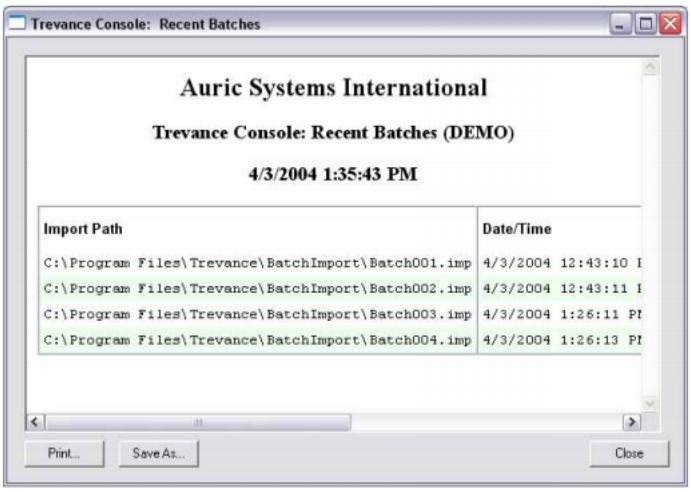
3. Type the company name. (The default is the user name.)
4. Click on

Change the heading at any time by repeating these steps before you print the report.

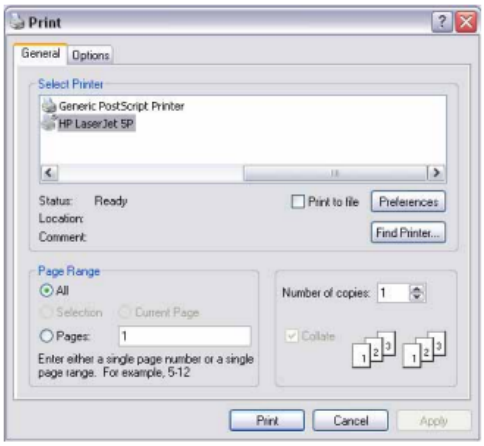
10.1.2 Printing Reports

To print a report (the page you're viewing):

1. Click on Reports.
2. Click on Print This Page to view a sample report. (If you're viewing the Batch screen, Trevance® asks if you want a report on the Submittal Queue or on Recent Batches.) You'll view a screen like the following:



Click on to view a screen like the following:



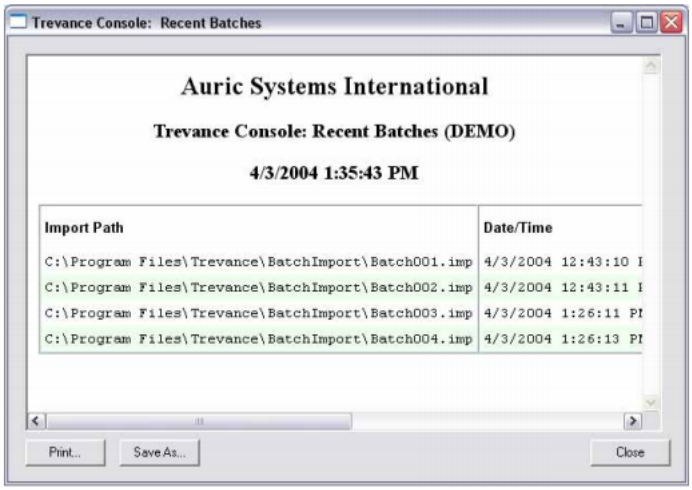
3. Click on

10.1.3 Saving Reports

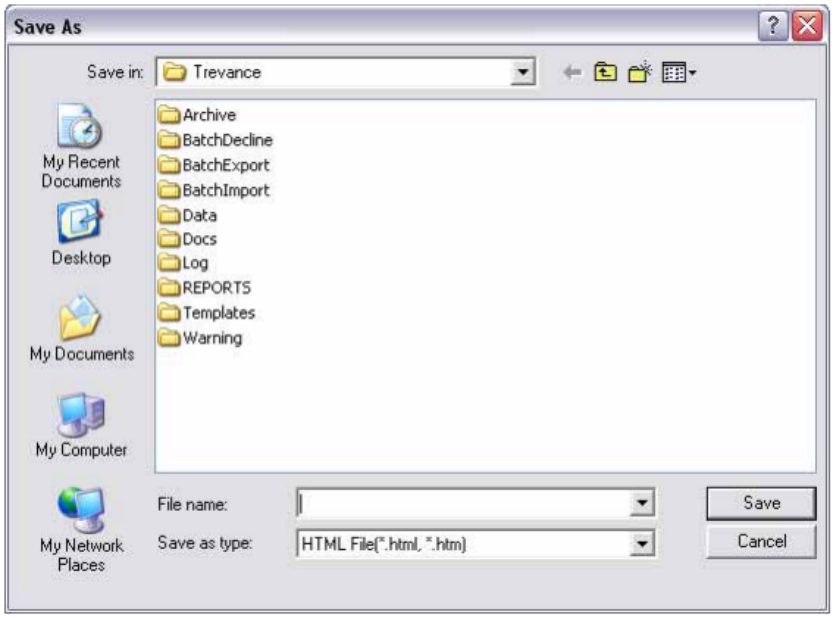
Any report can be saved in HTML format.

1. Click on Reports.

2. Click on Print This Page to view a sample report. (If you?re viewing the Batch screen, Trevance® asks if you want a report on the Submittal Queue or on Recent Batches .) You'll view a screen like the following:



3. Click on to view a screen like the following:



4. Select the place where you want to save the file (Save in) and type in the File name:.

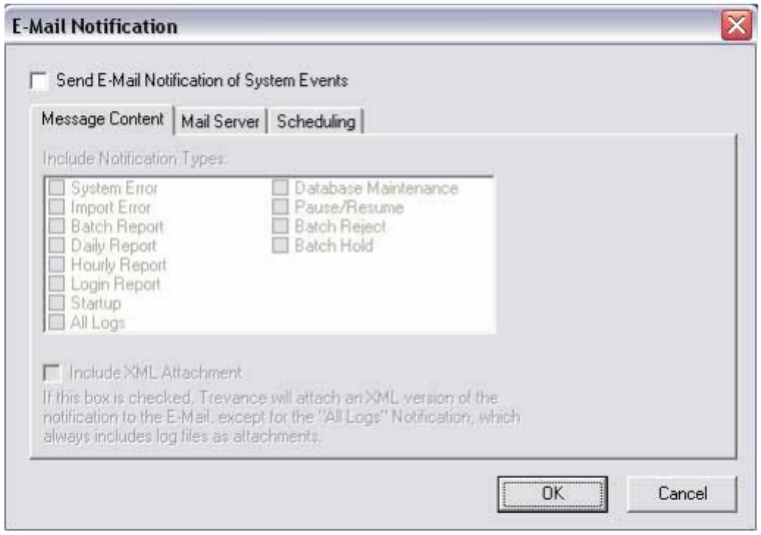
5. Click on

10.2 Configuring and Sending E-Mail Notifications (Messages)

At your request, Trevance® automatically sends you e-mail notifications of system events such as system errors, status of batches, the total value of authorization transactions, and who has logged in to the system.

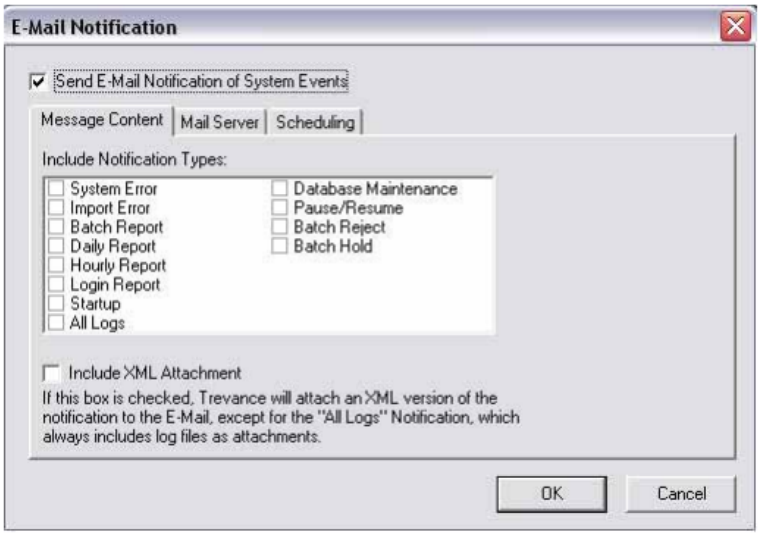
1. Click on Configure.

2. Click on E-Mail Notification to view:



The default is that no notifications are sent out.

3. To change the default, click on Send E-Mail Notification of System Events to view:



4. Click next to any messages you desire:

Table 10.1: Email Notifications

Type of Notification	*Contents*
All Logs	Delivers a copy of all logs as an attachment to the e-mail.
Batch Hold	Notifies you if the processing service sends a message that they are holding your batch. (Currently available with custom processor installations only.)
Batch Reject	Notifies you if the processing service rejected your batch. (Currently available with custom processor installations only.)
Batch Report	Summarizes information on successful batches, including types of transactions and total amount.
Daily Report	Lists all system activity for 24 hours from the time you select (the default time is midnight); it contains all the information included in all the other reports.
Database Maintenance	Notifies you immediately when database maintenance is complete.
Hourly Report	Gives the total value of authorization transactions by division, up to and including the previous hour.
Import Error	Lists any errors that occurred when importing batches.

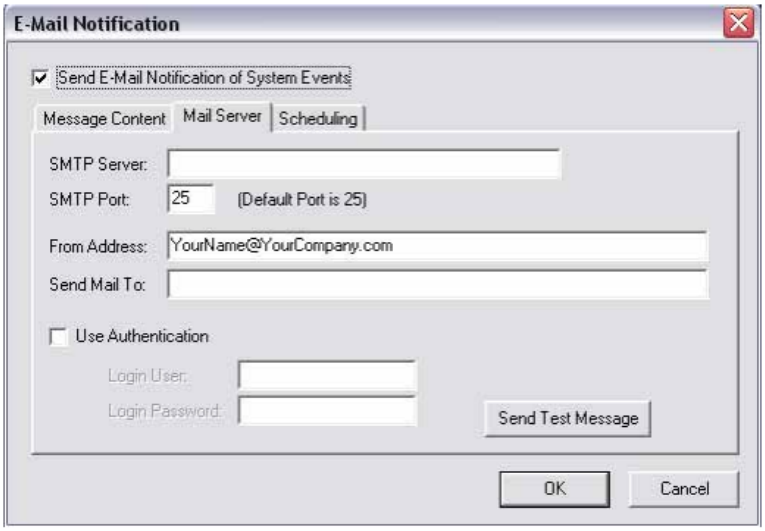
Continued on next page

Table 10.1 – *Continued from previous page*

Type of Notification	*Contents*
Login Report	Lists every log in, the time, and the IP the user logged in from.
Pause/Resume	Notifies you immediately whenever Trevance® is paused or resumed.
Startup	Notifies you immediately whenever the system starts up.
System Error	Lists any systems errors.

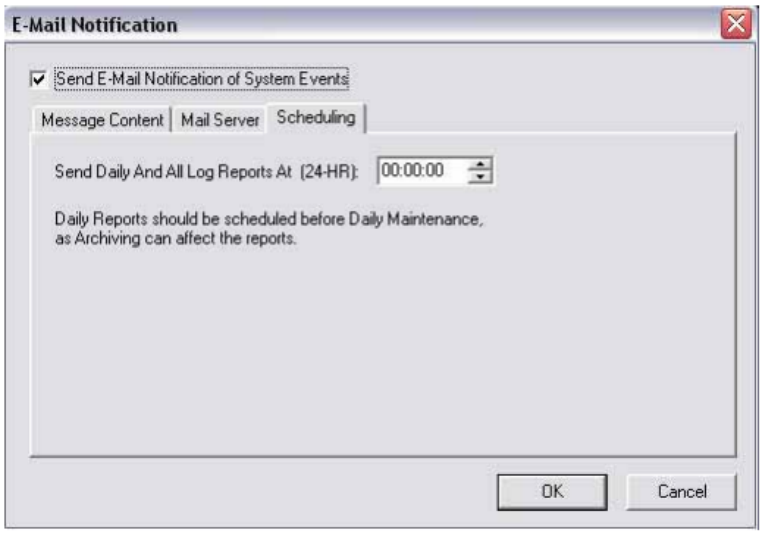
All e-mails also include information on the mode of Trevance® (demo, test, or production).

5. Click next to XML Attachment to automatically receive an XML version of the reports you selected.
6. Click on the Mail Server tab to view:



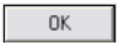
7. Type your SMTP Server address. You *must* enter an address before you can receive messages.

8. If necessary, change the SMTP Port. Auric Systems International strongly recommends that you leave the default at 25.
9. Type the Internet From Address. This is the address that appears in the "from" field of the e-mail you receive; you should select an address that identifies the e-mail as coming from Trevance® (say, trevance@example.com).
10. Type the e-mail Send Mail To address. Trevance® automatically sends the message to this address.
11. Click on Use Authentication to enter the userid and password of your e-mail server, if your e-mail system requires them. Trevance® then logs into the mail server using the account number and password you supply.
12. Click on Send Test Message to make sure e-mail is being sent and received properly.
13. Click on the Scheduling tab to view:



14. Change the time when you want to receive a Daily Report and/or an All Logs report. The default time is midnight (00:00:00).

    Daily reports should be scheduled before daily database maintenance (that is, before archiving occurs). For information on scheduling database maintenance, see Chapter 8.

15. Click on 

11 ACE: Auric Cipher Engine

All versions of Trevance® now support the Auric Cipher Engine™ (ACE) technology.

ACE is a standard interface from Trevance® (and CN!Express) to various third-party data encryption/decryption services. (ACE is also directly usable by any in-house merchant applications via a web service interface.)

The current ACE implementation communicates with custom in-house encryption/decryption services. ACE eventually will support a basic set of internal encryption/decryption and key management services as well as be integrated with off-the-shelf third-party tools.

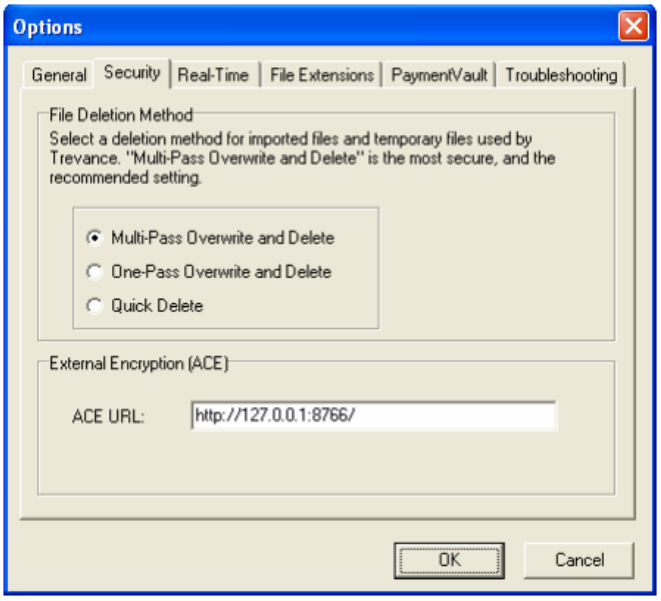
Please contact Auric Systems International for additional information and availability of ACE technologies.

11.1 Configuring Trevance® for ACE

The ACE settings allow you to set up ACE encryption/decryption support and connect to an optional external ACE server.

To configure ACE settings:

1. Click on Configure.
2. Click on Security.
3. Enter the full ACE url (could be http or https)
4. Click OK.



11.2 Using Encrypted Account Values

Trevance® (with ACE) provides a new Encrypted Account (EACCT) field. This EACCT field is used much the way the existing Account (ACCT) field is used.

To use ACE, a merchant typically configures Trevance® to export an Encrypted Account (EACCT) field and to accept both ACCT (for initial transactions) and EACCT (for subsequent actions) fields as input.

Typical data flow is as follows:

- Merchant process (web site, order entry system, etc.) sends Trevance® a transaction with a credit card (bank account, etc.) value in the ACCT field.
- Trevance® processes the transaction normally.
- At export time, Trevance® detects the request for an EACCT field. Trevance® sends the ACCT field value to ACE and waits for the encrypted response.
- Upon successful encryption, Trevance® returns the encrypted value in the EACCT field. The Merchant process can save

this encrypted value for later submissions. (see below for possible error responses).

- On subsequent submissions, the merchant process sends Trevance® the encrypted value in the EACCT field.
- Trevance takes the EACCT value and sends it to ACE for decryption.
- Upon successful decryption, Trevance® submits the transaction with the unencrypted account number to the processor.

11.3 ACE-Related Trevance® Error Messages

There are four encryption and decryption failure scenarios. Two for online (real-time web service) and two for batch.

11.3.1 Online Encryption Failure

The error is logged, but does not cause the transaction to fail.

Possible log messages:

- No server configured: "No Encryption Server to Encrypt Account"
- All other encryption failures: "ACE Encrypt Error: *specific ACE error*"

Response values:

- ACCT: Imported ACCT
- EACCT: Blank
- ASIRESP: According to primary transaction.
- RESPTEXT: According to primary transaction.

See below for specific ACE Errors.

11.3.2 Online Decryption Failure

Error causes transaction to reject.

Response values:

- ACCT: Blank
- EACCT: Imported EACCT
- ASIRESP: 311
- RESPTEXT: CNR – Local Reject Account Decrypt Failed: *msg*

  msg:
- No server configured: "No Decryption Server for Encrypted Account"
- All other decryption failures: "ACE Decrypt Error for EACCT *EACCT: specific ACE error"*

See below for specific ACE Errors.

11.3.3 Batch Encryption Failure

The error is logged, but the transaction is sent along in the batch.

Possible log messages:

- "ACE Encrypt Error: *specific ACE error"*

Response values:

- ACCT: Imported ACCT
- EACCT: Blank
- ASIRESP: According to primary transaction.
- RESPTEXT: According to primary transaction.

See below for specific ACE Errors.

11.3.4 Batch Decryption Failure

The transaction generates a warning that is written to the warning file. However, the transaction is still sent to the processor along with the other transactions in the batch. The error is also logged.

Warning strings (written to warning file):

- No server configured: "No Decryption Server for Encrypted Account"
- All other decryption failures: "ACE Decrypt Error for EACCT EACCT: specific ACE error"

Possible log messages:

- "ACE Decrypt Error: *specific ACE error*"

Response values:

- ACCT: Blank
- EACCT: Imported EACCT
- ASIRESP: According to primary transaction, but will be related to missing account number.
- RESPTEXT: Accoring to primary transaction, but will be related to missing account number.

See below for specific ACE Errors.

11.3.4.1 Specific ACE errors:

These are the specific ACE errors referenced above.

Errors Between Trevance® and ACE
ACE Server Timeout (for example, if ACE server not available): "Socket Error # 10060 Connection timed out."

Other socket errors will have a similar format.

Errors Returned by ACE Sever
Unknown Encryption Method: "01:Unknown Encryption Method"

ACE Error communicating with External Server: "90:*Server Error Text*"

Error returned by External Server: "92: *Server Error Text*"

12 4250 Features

The Trevance® CN-4250 contains several additional features, some of which are processor-specific:

- Real-time conditional deposit emulation (Chase Paymentech)
- Auto-settle (Chase Paymentech)
- ValueLink cards (Chase Paymentech)
- Disney Rewards cards (Chase Paymentech/PNS)

12.0.5 Real-Time Conditional Deposit Emulation

Except for ValueLink (Salem/Direct) and Disney Rewards Cards (Tampa/PNS), the Chase Paymentech real-time interface supports Authorization transactions only. It does not support Deposits or Refunds (and thus does not support Conditional Deposit (Sale) transactions which are a one-step Authorization and Capture).

The Trevance® real-time web interface supports these actions by capturing transactions for later batch settlement.

12.0.5.1 Deposits and Refunds

When Trevance®receives a real-time Deposit or Refund request through the web interface, it stores the transaction for later batch submittal and returns response codes indicating a successful transaction back through the web interface.

This success indicates only that the transaction has been stored for later submission. Until these transactions are presented to the processor, it is uncertain they will succeed. You must always check your batch export files to ensure they have all been successful.

If any of the Deposit or Refund transactions in a batch fail, you will receive an email notifying you of such. This is a reminder to check your exports when a transaction did not succeed.

12.0.5.2 Conditional Deposits/Sales

When Trevance® receives a Sale transaction, it sends an Authorization request to Chase Paymentech. If that Authorization succeeds, it then stores a Deposit request for later submission.

12.0.6 Settling Stored Transasctions

Trevance® provides three ways to submit the real-time transactions that are stored for later batch submission:

- Console Close Batch
- Web Command
- Auto-Settle.

IMPORTANT: When connected to Chase Paymentech, all three of these options submit transactions that were entered up to one hour before settlement time. Chase Paymentech requires transactions that were run through the real-time interface to not be settled for an hour. This allows their systems to communicate with each other.

12.0.6.1 Console Close Batch

You may manually send a settlement batch at any time.

- Start the Trevance® Console and log in.
- From the menu, select Configure/Options.

Note, you are not prompted with a confirmation dialog. Trevance® immediately creates a batch submission from any stored transactions that are at least one (1) hour old. This batch is soon uploaded.

This method is likely to be rarely used and is here to provide a simple way to settle during testing and certification.

12.0.6.2 Web Command

Trevance® accepts a web settlement command. You must first configure a web user to send commands.

From the Trevance® Console:

- Configure/Users
- Select or create a user account to which commands will be sent.
- User Type must be Web Interface
- On Privileges Settings tab, select Accept Commands from this User.

To create a settlement batch, POST the following command to the web interface:

COMMAND=batchclose&WEBUSER=user&WEBPASS=pw (where "user" and "pw" are replaced by the information you configured above) You will receive a two-field response:

- LAS (Last Action Succeeded)
- Response Message

These fields will be delimited or quoted according to the current web interface export settings.

Example response:

1|SUCCESS

12.0.6.3 Auto-Settle

You are able to optionally set a daily automatic settlement time for your batches.

From the Trevance® Console:

- Configure/Options/Real-Time tab.
- Check Automatically Settle Real-Time Transactions.
- Set an Auto-Settle time.

When auto-settle is enabled, Trevance® automatically sends a settlement request every day. Trevance® must be running at the requested settlement time.

12.0.7 ValueLink and Disney Rewards Cards

Trevance® supports Value-Link stored-value gift cards through the Chase Paymentech Direct Platform.

A custom CN-4250 version is available for processing Disney Rewards cards through the Chase Paymentech PNS Platform.

Please contact Auric Systems International regarding support for these specific payment types.

13 Monitoring

Trevance® provides a built-in monitoring service called Ping.

To use the monitoring

1. send a POST command to http://localhost:8004/PING
2. include the WebUser and WebPass fields
3. get back 200/Success response; or error if Trevance® is down.

14 Database Management

When using the embedded database, Trevance® creates a backup file during the normal daily maintenance. When using the remote database, you should perform a manual backup procedure on a daily maintenance basis. This backup file should be removed from the server and stored in a secure location as it is possible it contains encrypted credit cards.

Trevance® maintains Recovery Logs which contain the changes made to the database since the last backup. The combination of the database backup and the recovery logs allow you to recover the Trevance® operational state.

14.1 Restore

The restore tools are kept in the repair directory that by default installs at
`c:\AuricSystems\Trevance\repair`.

To restore a backup:

1. stop Trevance®.
2. locate the Data directory (default: `c:\AuricSystems\Trevance\data`).
3. rename the prod.fdb file to prod-old.fdb.
4. copy the latest backup (.gbk) file to the repair directory and rename it prod.gbk.
5. run the restore command:

   ```
   gbak -c -user userid -password passwd prod.gbk prod.fdb
   ```

   (contact tech support for the userid/password of the embedded system)
6. move the prod.fdb file into the data directory.
7. start Trevance®.

14.2 Recover

In order to recover the transactions created since the last backup was made:

1. copy all the files in the `RecoveryLog\PROD` directory of the old Trevance® installation to the new installation.
2. start the Trevance® Console and log in as the administrator.
3. pause Trevance®.
4. select File/Restore from Recovery Log.
5. restart Trevance®.

14.3 High Availability

When running in a high-availability environment, it is usual to have two load-balanced Trevance® installations in production paired with to load-balanced Trevance® installations in the fail-over or disaster recovery environment.

Prudent practice is to periodically copy over the contents of the Recovery Log from the production to the fail-over machine. As noted above, the combination of a backup and recent Recovery Logs provides the ability to restore the state of the Firebird database.

14.3.1 Copying Recovery Logs on Windows

In a high-volume environment, the copy logs are continually being written. As such, it can be difficult to get a clean copy of them. Performing just a simple copy or using an application such as RoboCopy will end up with many warnings that files are locked and unable to be written or moved.

In Windows, the correct way to address this problem is to take a Volume Shadow Copy before performing the copy operation. This takes a snapshot of the state of the files at a specific point in time and allows Trevance® to continue appending to these files while the copy is in process.

There are various administrative tools for performing this shadow copy. The instructions provided below are just one approach and uses RoboCopy to perform the actual copy operation.

1. Acquire a copy of vshadow: `http://msdn.microsoft.com/en-us/library/bb968832(v=vs.85).aspx`

2. Acquire a copy of dosdev: http://sourceforge.net/projects/vscsc/files/utilities/dosdev.zip/download
3. Find the vsrc.cmd file in the Trevance® repair directory.
4. Call vsrc.cmd like this: vsrc.cmdC:\AuricSystems\TrevanceServer[pathtobackupfiles]

14.4 Repair

It is rare to run into a corrupt Firebird embedded database. The specific areas where we've seen this occur with any of the payment applications is when a server runs out of disk space. You should always monitor your disk space on a regular basis and ensure your logs and backup files are being properly maintained.

If you should end up with a corrupt database, there's several steps that you can take to recover. The necessary tools are provided as part of the general Trevance® installation.

14.5 Windows®

All recovery work is done from the command line. The Trevance® installation includes a repair directory that by default installs at `c:\AuricSystems\TrevanceData\repair`.

1. If you are running the default embedded database, shut down Trevance® and make a copy of the database (prod.fdb). Call it prod-orig.fdb. Copy the prod-orig.fdb file to the repair directory.
2. From the command line, run the following command:

   ```
   gfix -v -f -user userid -password passwd prod-orig.fdb
   ```

   You should see errors reported.

   Note: Contact Auric Systems International tech support for userid/password.
3. Run the following command to prepare the database for recovery.

```
gfix -mend -user userid -password passwd prod-orig.fdb
```

4. Now back up the database:

   ```
   gbak -b -g -user userid -password passwd prod-orig.fdb prod-orig.fbk
   ```

5. Now restore it as good:

   ```
   gbak -c -user userid -password passwd prod-orig.fbk prod-good.fdb
   ```

6. Check to see there are no problems:

   ```
   gfix -v -f -user userid -password passwd prod-good.fdb
   ```

   You should not see any errors. If there are errors, contact Auric Systems International technical support for further instructions.

7. Shut down Trevance®. Rename prod.fdb to prod.fdb.bad
8. Copy prod-good.fdb to the data directory.
9. Rename prod-good.fdb to prod.fdb.
10. Restart Trevance®.

Part II

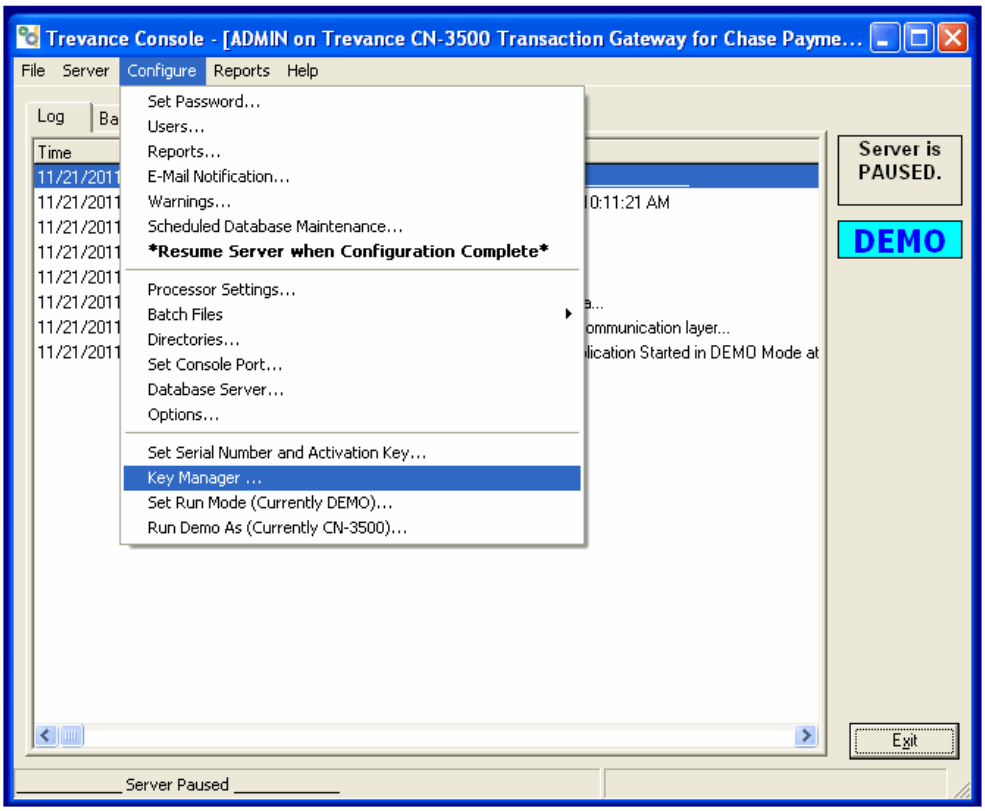
External Key Management

15 akmp

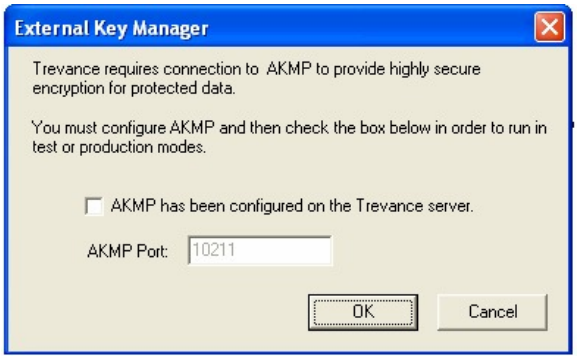
Trevance® supports external key management services. The various key management services are supported via the Auric Key Management Proxy or AKMP™. The AKMP™ allows new key management services to be added without needing to update the basic Trevance® application. AKMP™ is installed on your system and is part of the basic Trevance® installation.

The AKMP™ is not required to be configured for Demo mode. In demo mode, Trevance® uses a hard-coded demo encryption key since you are only using demo account numbers. When you are ready to move to test (and production), refer to the instructions below:

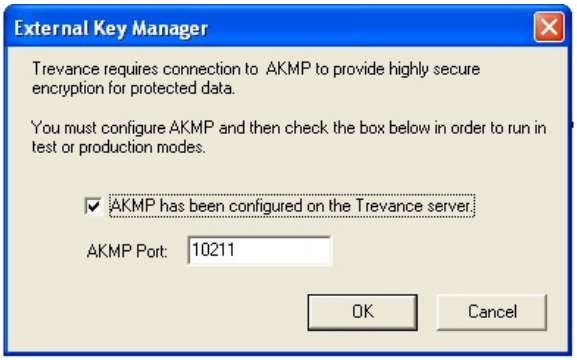
1. Select Configure followed by Key Manager



2. Click AKMP has been configured on the Trevance server


External Key Manager
Trevance requires connection to AKMP to provide highly secure encryption for protected data.
You must configure AKMP and then check the box below in order to run in test or production modes.
AKMP has been configured on the Trevance server.
AKMP Port:
10211
OK
Cancel

3. Click OK


External Key Manager
Trevance requires connection to AKMP to provide highly secure encryption for protected data.
You must configure AKMP and then check the box below in order to run in test or production modes.
AKMP has been configured on the Trevance server.
AKMP Port:
10211
OK
Cancel

4. Your External Key Manager is now active

Part III

Payment Processors

16 Chase Paymentech Solutions Direct/Salem

This chapter contains information on configuring processor settings specifically for the Chase Paymentech Solutions (Paymentech) Direct platform, sometimes referred to as "Salem".

Paymentech maintains redundant Direct processing facilities in their Salem, NH, and Tampa, FL, facilities.

Trevance® CN-3500 (batch only) communicates with Paymentech Direct via SFTP (secure Internet), VPN, or Frame Relay.

Trevance® CN-4200 communicates with Paymentech Direct via VPN or Frame Relay. Both VPN and Frame Relay provide highly reliable communication and rapid transaction turn-around times. Paymentech states that real-time transactions reliably process in 3 to 4 seconds.

Trevance® provides a built-in failover functionality. Paymentech can provide merchants with additional network-level redundant failover configurations. Please contact your Paymentech representative for details.

Trevance® supports both the Paymentech On-Line (real-time) Authorization service and FTP batch processing service. Please refer to the Trevance® README file to determine the latest Paymentech specification to which Trevance® has been certified.

If using SFTP Batch connection to Chase Paymentech, please refer to the *Trevance® Automated Password Updates for Chase Paymentech Solutions Net Connect Batch (SFTP)* document.

For additional documentation, see the Auric Systems International web site, specifically:

- *General Trevance® Support*

  `http://www.AuricSystems.com/support-center/trevance`

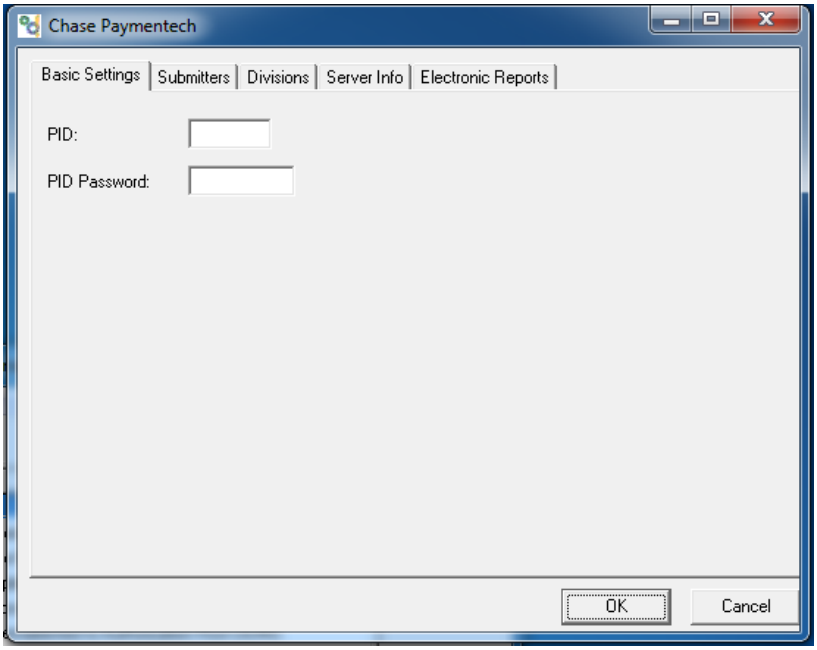
Additional .html reference documents are available your local Trevance® Doc directory.

You may also find Paymentech's 120-byte *Batch Technical Specification* and *On-Line Processing Technical Specification* to be useful. Please contact your Paymentech representative for copies.

Configuring Processor Settings

To configure the processor settings:

1. Click on CONFIGURE.
2. If the server isn't paused, click on *PAUSE SERVER TO CONFIGURE ITEMS BELOW*.
3. Click on PROCESSOR SETTINGS to view a screen like the following:



The screen, tabs, and boxes that you see are set up specifically for Paymentech Gateway. Paymentech provides you with the documentation required to complete this configuration.

16.0.1 Basic Settings

4. Click on the BASIC SETTINGS tab.

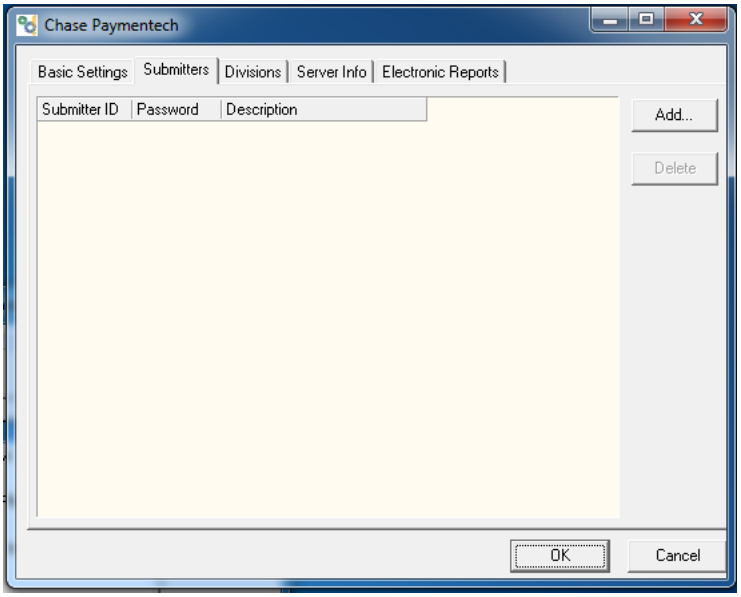
   BASIC SETTINGS information identifies the company presenting the transactions to Paymentech. In other words, it identifies the company that is running Trevance®.

This is required information, which comes from Paymentech.

5. Fill in the PID (for batch transactions only). The PID (Paymentech presenter ID) identifies your installation.
6. Fill in the PID PASSWORD (for batch transactions only). This is the password associated with the Paymentech presenter ID.

16.0.2 Submitters

7. Click on the SUBMITTERS tab to view a screen like the following:



The SUBMITTER ID and PASSWORD are necessary for batch transactions only. They identify the company whose transactions are being submitted to Paymentech. Frequently, the presenter and submitter companies are the same; however, they may be different for third-party submitters, such as in-bound call centers.

At least one submitter is required.

Most installations now use a single submitter ID, even if they are an in-bound call center processing for dozens of

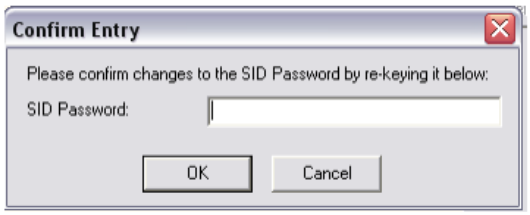
clients. Support for multiple submitters is mostly for historic purposes.

The submitters grid is sortable. Click on a heading (SUBMITTER ID, PASSWORD, DESCRIPTION) to change the sort order.

8. To add a submitter, click on

9. Type a number into the Submitter ID box. This number is supplied by Paymentech and must be entered exactly as supplied. It identifies the company submitting the transactions.

10. Type a password into the PASSWORD box to view:



This is the password associated with the submitter ID (SID).

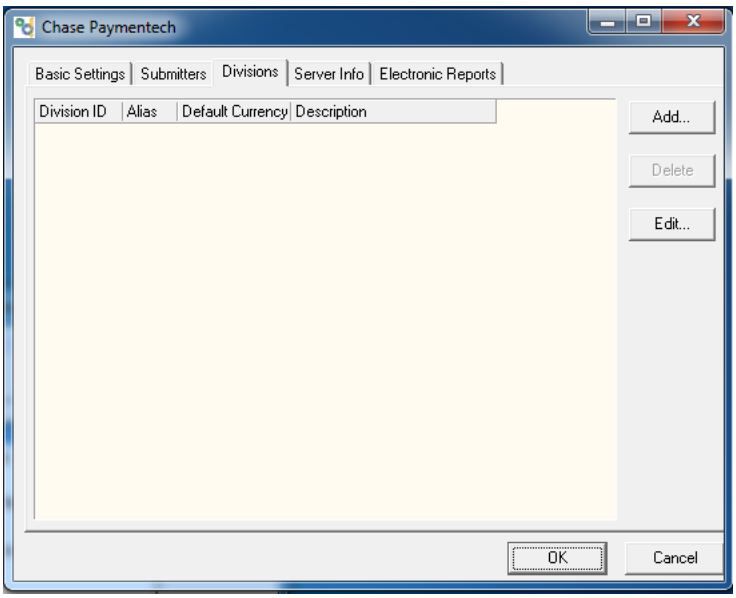
11. Re-enter the password.

12. Click on

13. Enter a DESCRIPTION. This description is for your own use in identifying the submitter. The description is never sent to Paymentech.

16.0.3 Divisions

14. Click on the DIVISIONS tab to view a screen like the following:



Divisions identify transactions as belonging to different categories, such as the different parts of a large company, mail order/phone order/web sales, or totally different companies (as in the case of an in-bound call center processing for many merchants).

Divisions are also used to process and report on transactions in different currencies. Although Paymentech allows you to set the currency value with each and every transaction, it is typical, and considered a best practice, to have Paymentech configure a division for each currency in which you process.

You'll see this information again on when you configure import files. At that time, the division number(s) and associated description(s) are automatically listed under the DEFAULT VALUES tab (in the DIVISION ID box).

The divisions grid is sortable. Click on a heading (DIVISION ID, ALIAS, DEFAULT CURRENCY, DESCRIPTION) to change the sort order.

15. To add a division, click on

16. Type the division number under DIVISION ID. This 10-digit number is supplied by Paymentech and must be typed exactly as supplied. The number must have 10 digits; if you

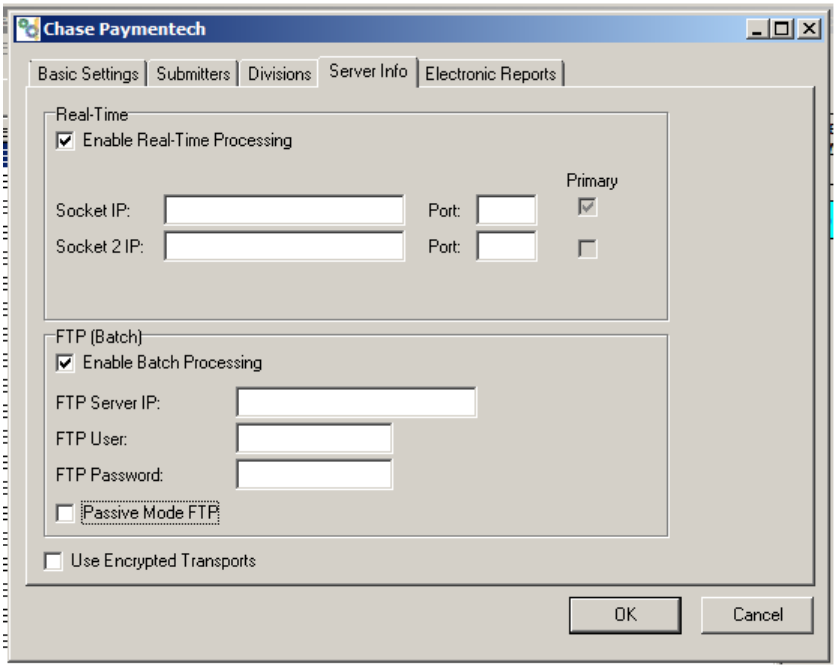
have an 8-digit number, add two zeroes to the left hand side (for example, change 12345678 to 0012345678).

17. The ALIAS field is provided for future functionality. Leave it blank for now
18. Under Default Currency, click on ··· to view a list of currencies.
19. Click on the currency you want. Trevance® automatically uses that currency for all transactions associated with that particular division ID.

    If you leave the field blank, U.S. dollars are used by default.
20. Enter a DESCRIPTION. This description is for your own use in identifying the submitter. The description is never sent to Paymentech.

16.0.4 Server

21. Click on the SERVER INFO tab to view:



The server information is used to configure communications with Paymentech.

The real-time and batch systems each have their own configuration.

Although most installations perform both real-time and batch operations, you can disable either one if you like. For example, if you already have a batch operation process in place, you can use Trevance® to add real-time operations while continuing to perform your existing batch actions.

22. Fill in the REAL-TIME (SOCKET) boxes based on information you receive from Paymentech. The IP fields are in the form of "dotted notation" (for example, 192.1.1.42). The real-time interface has a separate socket.

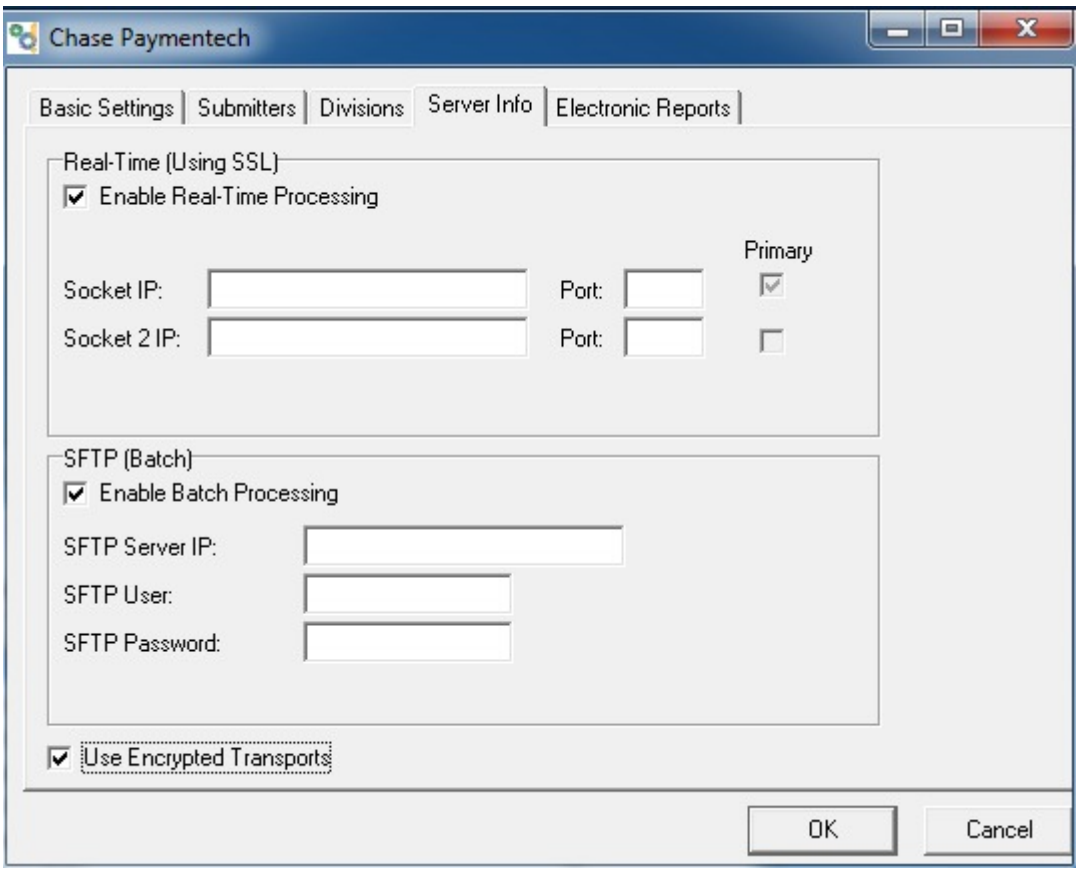
    Suppose Paymentech provides an address that looks like this: 192.1.1.42:8443.

    - In the SOCKET IP, type 192.1.1.42.
    - In the SOCKET PORT, type 8443.

23. Trevance® allows you to optionally configure a primary and failover Socket IP. This allows you to configure one connection communicating with Chase Paymentech's Salem facility and one communicating with Paymentech's Tampa facility. If you are not configuring failover capabilities, enter only the first Socket IP value.

24. Select Primary Socket Connection. This defaults to the first Socket IP address. If you want to select the second as your primary, click the checkbox next to the Socket 2 IP field.

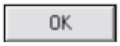
25. Fill in the FTP (BATCH) boxes based on information you receive from Paymentech.



26. For encrypted transport through SFTP, check the "Use Encrypted Transports" box, then fill in the boxes based on information provided by Paymentech.

    Both Real-Time and Batch connections are encrypted.

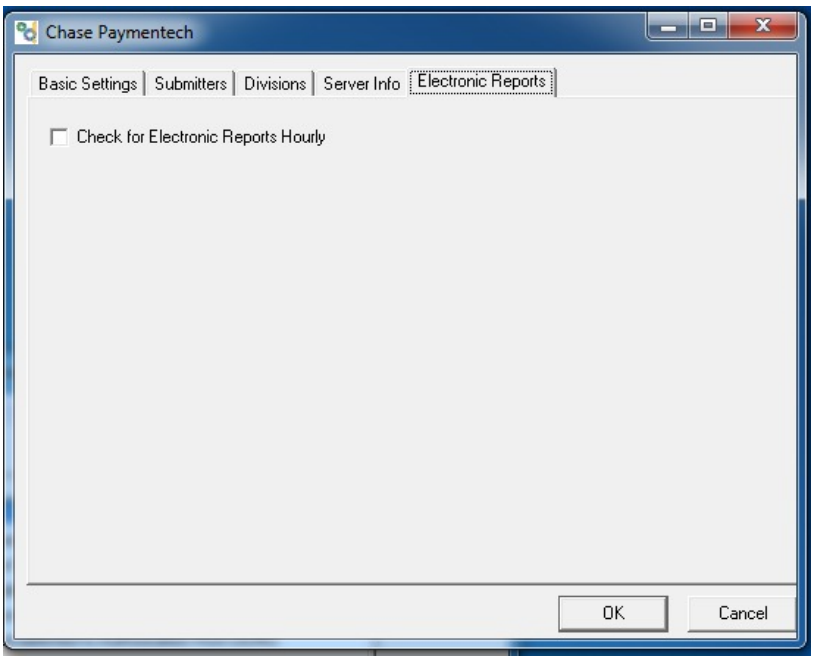
    For SFTP using the 3250, see "NetConnect" section, below.

27. Click on 

    Check your import and export formats to make sure they're using the information you just entered.

16.0.5 Electronic Reports

Click on the ELECTRONIC REPORTS tab to view:



Paymentech provides the ability to pick up what they refer to as delimited file reports or "DFR" (sometimes referred to as electronic reports). This area in the configuration of Trevance® enables Trevance® to pick up those files on an hourly basis.

16.0.6 How Failover Works

The Trevance® failover mechanism works as follows:

- When two Socket IP connections are defined, Trevance® uses one as the Primary and one as the Secondary.
- The Primary Connection is indicated by a checkmark in the Server Configuration screen (see above).
- All real-time transactions are sent to the Primary Connection.
- If the Primary Connection is unavailable (disconnected), Trevance® switches to sending transactions to the Secondary Connection.
- If a real-time transaction is sent and never received because the socket disconnects, Trevance® eventually times-out the

transaction and returns with a timeout error. Trevance® **does not** automatically retransmit the transaction. The decision to retransmit a real-time transaction is left as a business decision on the merchant side. Retransmitting some transactions (such as debit card authorizations) have monetary consequences.

- If a transaction timeout is received, Trevance® switches connections.

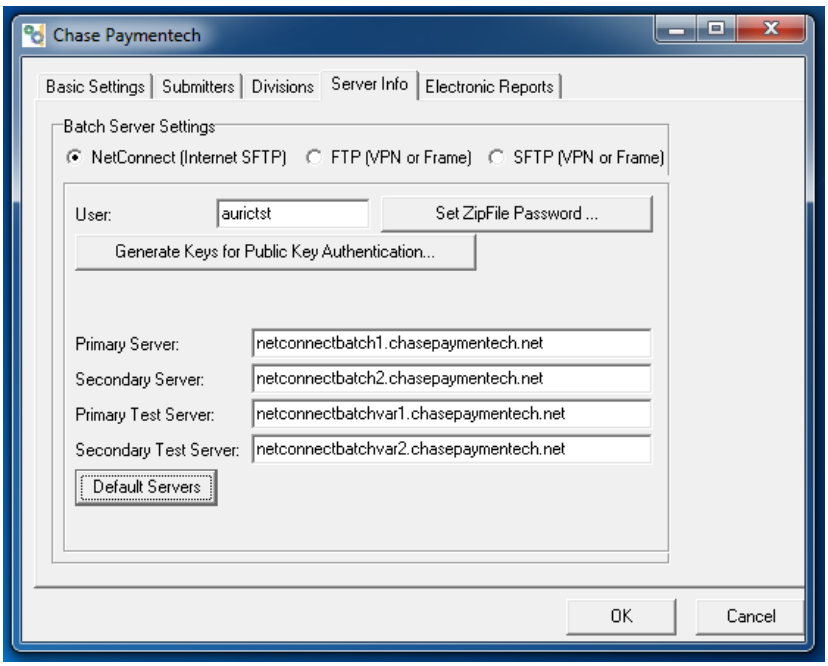
- Primary socket connection can also be set manually without pausing Trevance® Select Server/Primary Real-Time Socket from the menu and select which socket you want to use as the Primary socket.

- A log entry appears whenever connections are switched.

16.0.7 S-FTP Server with NetConnect

The Trevance® CN-3500 supports S-FTP over Internet as well as FTP over Frame Relay/VPN. Please check with your Paymentech representative regarding this ability.

In the CN-3500, The Server Info tab provides a radio button for selecting between NetConnect (Internet SFTP) FTP (VPN or Frame) and SFTP (VPN or Frame) When you choose use NetConnect (SFTP), Trevance® presents the following dialog



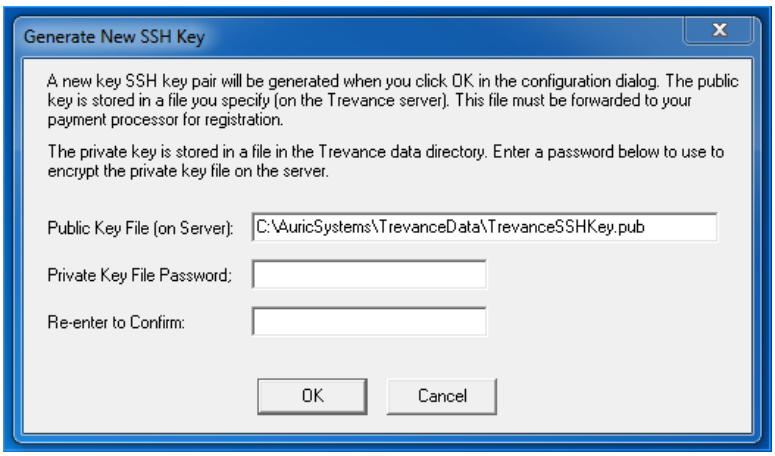
The information for completing these fields is provided by Chase Paymentech. Never enter information here that is not provided by Chase Paymentech.

Complete the fields as follows:

User: S-FTP user login name provided by Chase Paymentech.

Set ZipFile Password: ZipFile password provided by Chase Paymentech

Generate Keys for Public Key Authentication: This will generate new SSH key pair:


Generate New SSH Key
A new key SSH key pair will be generated when you click OK in the configuration dialog. The public key is stored in a file you specify (on the Trevance server). This file must be forwarded to your payment processor for registration.
The private key is stored in a file in the Trevance data directory. Enter a password below to use to encrypt the private key file on the server.
Public Key File (on Server):
C:\AuricSystems\TrevanceData\TrevanceSSHKey.pub
Private Key File Password:
Re-enter to Confirm:
OK
Cancel

Enter a private key file password

The public key will be stored in the TrevanceData folder

The private key will be store in the TrevanceData/data folder

Forward the public key to your Paymentech representative

Once the key is "loaded up" and you're given the ok by your Paymentech representative, you're ready to proceed

Servers: Primary and secondary test servers. Click the Default Servers button to fill in the default values.

See the following section *How NetConnect Passwords Work* for details as to how Trevance® automatically handles the S-FTP and the encryption passwords for you.

You are now set to communicate with Chase Paymentech's NetConnect Batch system. During your certification run, Chase Paymentech will ask you to send a password change request. They may ask for you to send an xml password changefile. Click the Test 30-day Password Change... button. When you resume Trevance® , it will send the NetConnect password change request.

16.0.8 How NetConnect Passwords Work

NetConnect batch communication requires a user id and two passwords:

- the S-FTP connection password
- the .zip file encryption password (key)

Since initially these are set to the same value, Trevance® requests only a single password be entered

Chase Paymentech requires the S-FTP password be periodically changed. Trevance® supports automatic password updates for NetConnect batch using Chase Paymentech's automated password change request. Trevance® automatically changes the password every 30 days.

During testing, Chase Paymentech will ask you to test the 30-day change capabilities. Just click the "Test 30-day Password Change..." button and then resume Trevance® .

16.0.9 Merchant Perspective

Because Trevance® handles password changes automatically, the merchant does not know the password once the first password change occurs (30 days after installation, or during certification when you click the Test button). Should the merchant need to reinstall Trevance® , or otherwise need to know the current password, they must call Chase Paymentech and request a manual password reset.

With a manual password reset, Chase Paymentech support generates a new password and gives it to the merchant. The merchant must then enter the password into the password box in the Trevance® console. Once the password change takes effect (manual reset can take up to two hours), Trevance® is able to connect to Chase Paymentech using the new password.

Manual password reset is not recommended except for reinstallation or other recovery methods; it should not be used on a regular basis. Except for manual reset, the merchant should not change the password using Trevance® console. In particular, the user may not enter an arbitrary new password. The new password must be supplied by Chase Paymentech in the manual reset process.

16.0.10 Implementation Details

Under the hood, there are actually two passwords:

- The SSH login password.

- The Zip file password (batches are sent and response files received in encrypted zips.

Automatic password updates, and the 30-day expiration, apply only to the SSH login password, not the zip file password. However, a manual reset changes both the Zip file password and the SSH login password.

Trevance® maintains the following information in the database:

- The current S-FTP password.
- The current Zip password.
- The last working S-FTP password.
- The date and time when the password was last changed (manual or automatic).

Whenever Trevance® successfully logs into the S-FTP server, it updates the last working S-FTP password to the password used to log in.

While running, Trevance® checks at regular intervals to see if the password was last changed 30 or more days previous. If it was, Trevance® does the following:

1. Automatically generates a new password that conforms to Chase Paymentech password rules.
2. Sends a password change request file to Chase Paymentech.
3. Sets the current S-FTP password to the new password.
4. If no last working S-FTP password was recorded, set the last working S-FTP password to the old S-FTP password.

Note that this does not affect the Zip file password.

The password change takes a few minutes to take effect, and will either succeed or fail (it should generally succeed, as we are following all of the timing and formatting rules). If it succeeds, the password will change, but there will be no notification. If it fails, the password will not change, and there will be, at some point, a notification file in the download directory.

Trevance® always attempts to log in first with the current S-FTP password; if that fails, it then tries the last working S-FTP password. That means that whether the change succeeds or not, and regardless of the timing at which the change takes effect. Trevance® will be able to log in.

If, during the course of normal operation, Trevance® finds a password error file, it downloads the file, displays the error message in the log, and then undoes the internal password change. Specifically, it swaps the current S-FTP password and the last working S-FTP password. This means that the same two passwords are available to try, although now the "old" working password is tried first.

If this occurs, Trevance® also immediately sets the last change date to a date 31 days in the past, so that a new password change attempt is generated.

Chase Paymentech requires that passwords are never re-used. Rather than track all passwords ever used, Trevance® relies on the unlikeliness of a duplicate ever being generated (there are around 64 8 possible generated passwords), and its ability to handle password change error files and re-issue password change requests should a duplicate occur.

For a manual reset, the merchant must contact Chase Plummeted and enter the given password into Trevance® console. When this occurs, Trevance® sets the S-FTP password and the Zip password to the new value, deletes the previous S-FTP password values, and updates the last password change date.

16.0.11 NetConnect Batch Password Summary

In short, once you've entered the initial NetConnect password information, Trevance® handles all the automated 30-day password updates for you.

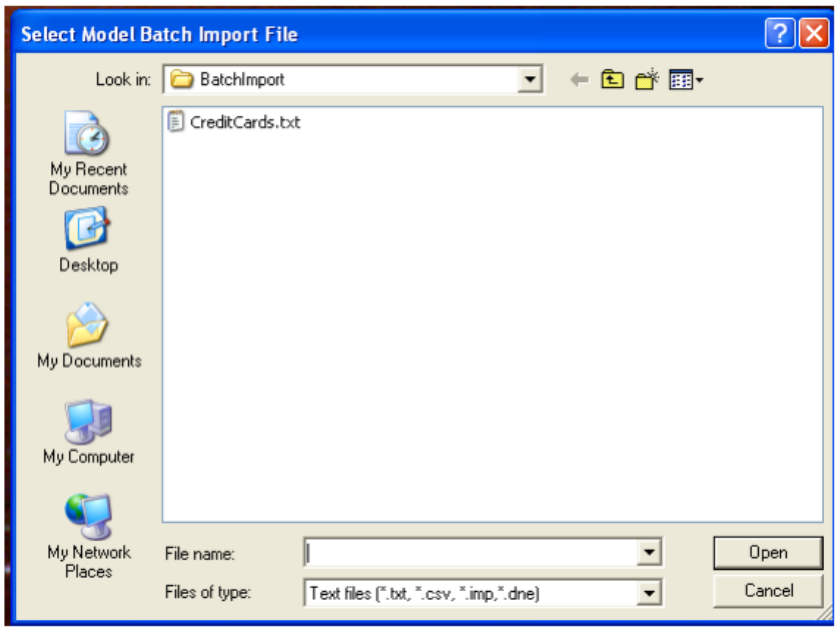
Configuring Transaction Defaults

This section covers Paymentech-specific details of batch file and realtime web configuration.

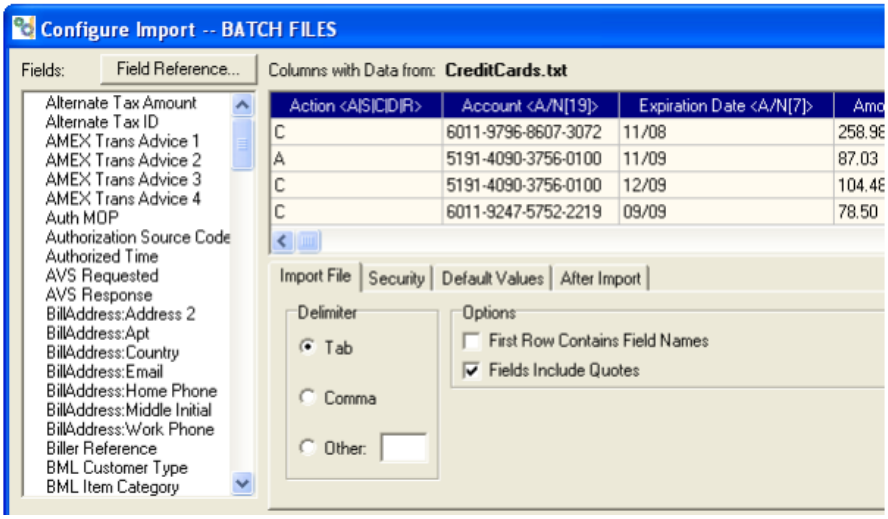
16.0.12 Configure Import Defaults for Batch Files

Refer to "Configuring Imports for Batch Files" on page 61 for general information about import configuration.

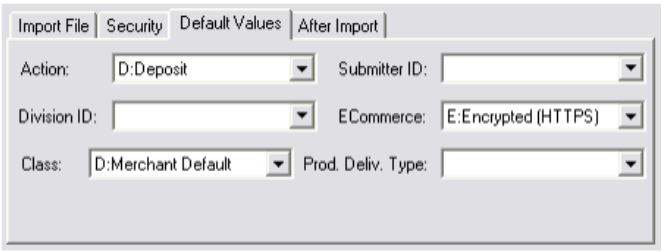
1. Click on CONFIGURE.
2. If the server isn't paused, click on *PAUSE SERVER TO CONFIGURE ITEMS BELOW*.
3. Click on BATCH FILES.
4. Click on BATCHIMPORTS to view:



5. Select the sample CREDITCARDS.TXT file (or any file of your own that you're using for import configuration) to view:



6. Click on DEFAULT VALUES to view:



This screen lets you select default information for Trevance® to use with the transaction if certain fields are missing.

- ACTION for real-time file transactions: AUTHORIZATION is the only action accepted by Paymentech (and Trevance®) through their system. If you are handling a PIN-based debit, you can send a real-time REFUND AUTHORIZATION (RA) transaction. This is considered to be a type of "authorization": a refund authorization.

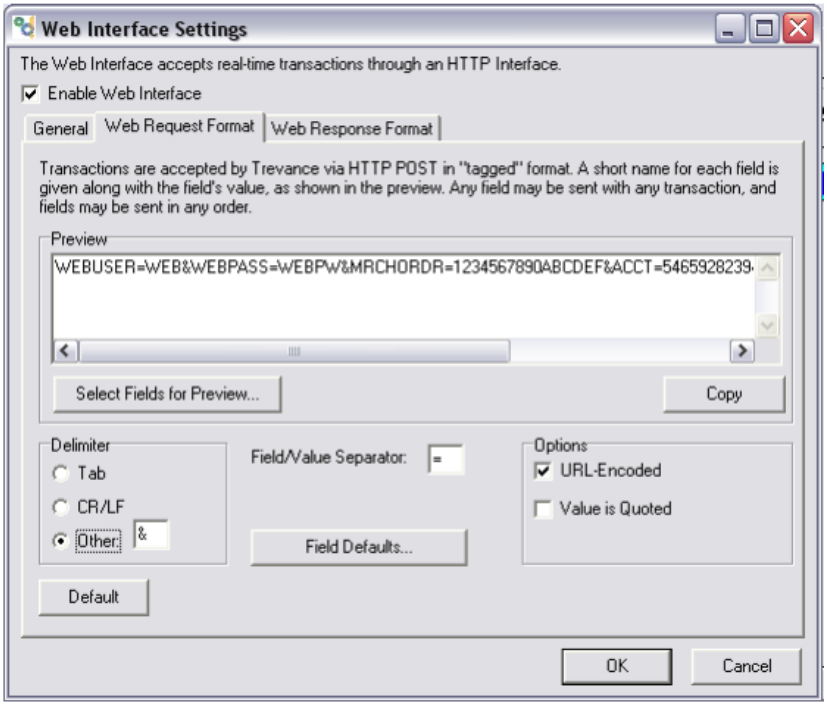
- ACTION for batch transactions: The two most common default actions are AUTHORIZATION and SALE (also known as conditional deposit).

- DIVISION ID: This is the Paymentech division ID that is assumed for all transactions submitted with a division.

- SUBMITTER ID: Batch only. Most current installations have a single submitter ID for all transactions. Select that submitter ID.
- CLASS: Many merchants have Paymentech assign a specific transaction class to each division. Select MERCHANT DEFAULT to use the Paymentech configuration.
- PRODUCT DELIVERY TYPE: Optional field. Leave it blank if you're not sure how to fill it in.
- ECOMMERCE: This field describes the method by which ecommerce transactions are received. The most common is ENCRYPTED (HTTPS), indicating a secured web transaction. You can set a different default value at Paymentech for each division. If you use that method, select MERCHANT DEFAULT.

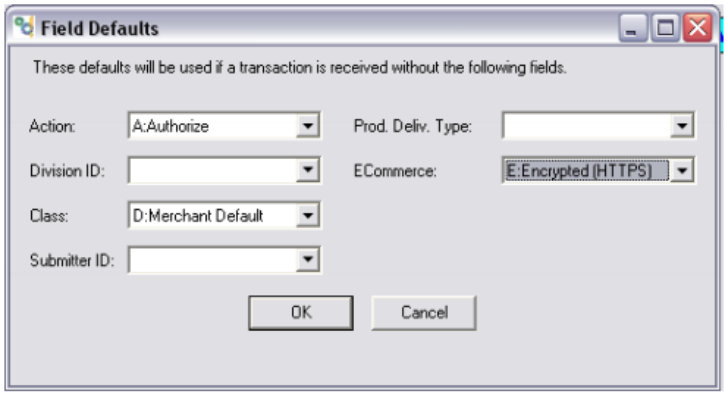
16.0.13 Configure Web Transaction Defaults

Refer to "Configuring the Real-Time Web Interface" on page 80 for general information on web transaction configuration.



1. Click on CONFIGURE.
2. If the server isn't paused, click on *PAUSE SERVER TO CONFIGURE ITEMS BELOW*.
3. Click on REAL TIME WEB INTERFACE, then the WEB REQUEST FORMAT tab to view:
4. Click on

to view:



This screen lets you select default information for Trevance® to use with the transaction if certain fields are missing.

- ACTION: AUTHORIZATION is the only action accepted by Paymentech (and Trevance®) through their real-time or on-line system.

  If you are handling a PIN-based debit, you can send a real-time REFUND AUTHORIZATION (RA) transaction.This is considered to be a type of "authorization": a refund authorization.
- DIVISION ID: This is the Paymentech division ID that is assumed for all transactions submitted with a division.
- SUBMITTER ID: Most current installations have a single submitter ID for all transactions. Select that submitter ID.
- CLASS: Many merchants have Paymentech assign a specific transaction class to each division. Select MERCHANT DEFAULT to use the Paymentech configuration.
- PRODUCT DELIVERY TYPE: Optional field. Leave it blank if you're not sure how to fill it in.

- ECOMMERCE: This field describes the method by which ecommerce transactions are received. The most common is ENCRYPTED (HTTPS), indicating a secure web transaction. You can set a different default value at Paymentech for each division. If you use that method, select MERCHANT DEFAULT.

Methods of Payment, Actions, and Required Fields

Trevance® for Paymentech Direct supports the following methods of payment (MOPs):

- Credit card: American Express, Carte Blanche, ChaseNet, Delta, Diners Club, Discover, JCB, MasterCard, Novus, Optima, Visa
- Purchase card (level II): American Express, MasterCard, Visa.
- Purchase card (level III): MasterCard, Visa
- Electronic checks: via the Web, Point of Purchase (POP), and Accounts Receivable Conversion (ARC).
- Switch/Solo/Maestro: UK private label debit card
- Third-party encrypted credit card
- Third-party encrypted check
- PIN-less debit card
- PIN-based debit car
- Bill Me Later®
- Green Dot®MoneyPak
- PayPal ®
- European debit
- ValueLink (custom CN-4250)

Trevance® automatically recognizes some of these methods of payment. For others, specific fields must be set. Refer to the

"Method of Payment" documentation in the *Trevance® Field Reference for Paymentech Direct* (http://www.AuricSystems.com/trpaymentech120).

Important Information about Debit Cards

Debit cards are *not* credit cards. Debit cards must be treated in a significantly different way from credit cards.

The following table lists the most important information about debit cards.

Table 16.1: Chase Paymentech Salem - Debit Card

Item	*Applies to PIN-Less*	*Applies to PIN-Based*
"Authorizing" a debit card automatically removes money from the customer's checking account into Paymentech's.	yes	yes
You cannot reverse this"authorization"	yes	no
A "refund authorization" automatically adds money to the customer's checking account.	no	yes
"Depositing" a debit card moves money from Paymentech's account into your account.	yes	yes
You cannot "void" a debit authorization.	yes	no
You cannot "Auth for a dollar" to verify the debit card is valid. If you try to "Auth for a dollar," you remove $1.00 from the customer's checking account.	yes	yes
You must deposit the exact same amount as you authorized.	yes	yes
If you authorize a debit transaction, the money is removed from the customer's account; but then you have to deposit the "authorized" transaction to put the money in your account. If you don't deposit, the money won't be put into your account.	yes	yes

Continued on next page

Table 16.1 – *Continued from previous page*

Item	*Applies to PIN-Less*	*Applies to PIN-Based*
There is no SALE transaction type–only real-time authorization followed by a batch deposit.	yes	no
There is no REFUND transaction.	yes	yes
Authorization codes sometimes return as blank. This is valid behavior.	yes	yes
You can check the LASTACTIONSUCCEEDED or RESPONSE CODE field to determine if the authorization succeeded.	yes	no

16.0.14 Required Information

Regardless of the method of payment, Paymentech transactions require the following information:

- ACCOUNT: Credit card, debit card, or bank account number.
- ACTION: Authorization, sale, deposit, refund. Set to default or import with each transaction.
- AMOUNT
- DIVISION ID: Set to default or import with each transaction.
- MERCHANT ORDER NUMBER: Every transaction requires a merchant order number. This value is used for tracking transactions through Paymentech and the Card Associations.

  Merchants should provide a MERCHANT ORDER NUMBER with each transaction. Trevance® generates an order number if one is not provided. If you're performing two-pass authorization transactions that are followed by deposits, you must use the same order number for the deposit *and* for the authorization.

- PRESENTER ID and PASSWORD: Batch only. Configured in Trevance® and never imported.
- SUBMITTER ID and PASSWORD: Batch only. Usually set to a default value in Trevance® since it is rare to find someone using multiple submitter IDs. If you do use multiple submitter IDs, you must import the submitter ID with each batch transaction. All batch transactions must use the same submitter ID.
- TENDER TYPE: Credit card, purchase card, check, etc. For some transactions - those using credit cards, checks, or Bill Me Later - there's no need to import the tender type. It is a good practice to always import the tender type so you are prepared for new future payment methods that may require the field. The following tables indicate when it's necessary to import the tender type.

The following tables show the minimum additional information that you must send for each method of payment - not the information that results in your best interchange rate (processing fee). These tables assume you're sending the ACCOUNT, ACTION, AMOUNT, DIVISION ID, and (if necessary) SUBMITTER ID.

Performing basic credit card and check processing with Trevance® for Paymentech Direct is simple and can be set up quickly. Ask your Paymentech representative what is necessary for more complicated transactions.

16.0.15 Generally Useful Fields

The following fields are generally useful for most types of transactions. Refer to the on-line field reference list for additional information.

- CARDTYPE: differentiates between ChaseNet CZ (credit card) and CR (prepaid debit)
- COMMENT (1 through 4): Four 128-character general-purpose fields. Not sent to Paymentech. Use these for your own tracking purposes.

- CURRENCY: Usually set as a default at the division level and not imported.
- CUSTOMER IP ADDRESS: Useful for tracking and fraud purposes when processing e-commerce transactions.
- LAST ACTION SUCCEEDED: Returns "Y" whenever a requested transaction was successful. Otherwise, it returns "N." A useful first check to see if a transaction request was approved.
- RESPONSE CODE: Paymentech's three-digit response code.
- SOFT DESCRIPTOR (1 and 2): Provides information on the cardholder's monthly statement. This must be set up at Paymentech before you can use it.

In addition to the fields described above, you should also send the account holder's full name (FIRST NAME and LAST NAME fields) as well as the address, city, state, and ZIP or postal code whenever available. This helps reduce your interchange rate (processing fee). If you do not have a full address, at least obtain and send a ZIP code (U.S.) or postal code (Canada and United Kingdom).

Additionally, obtain and transmit the card security code (CVV2/CID) information with authorization transactions.

16.0.16 Advanced Configuration

The following tables show the basic transaction information for each type of transaction. Once you get beyond the basics, you must consult with your Paymentech representative to determine what data you should be sending for maximum efficiency and lowest processing fees (also called interchange).

Paymentech's *On-Line Processing Technical Specification* and Batch Technical Specification describe over 160 possible fields that can be transmitted. The specific fields you should send will depend on your market type, your business class (e-commerce, MOTO, recurring, IVR, retail, and so on), and the forms of payment you accept (credit card, purchase card, check, debit, Bill Me Later, ARC, POP, and so on). Working with your Paymentech representative is the quickest way to determine which fields you should send.

Table 16.2: Chase Paymentech Salem - Credit Card

Authorization	*Auth Reversal*	*Deposit*	*Sale*	*Refund*
Exp Date	Exp Date	Exp Date	Exp Date	Exp Date
	Auth Date	Auth Date		
	Auth Code	Auth Code		

Account Check	*PartialAuth*	*Force Full Auth*
Exp Date	Exp Date	Exp Date

Transactions that contain the minimum information plus an expiration date are automatically identified as "credit card" transactions. Sending a "C" in the TENDER TYPE field explicitly identifies credit card transactions.

Credit card account values can contain spaces or dashes ("-"). Paymentech recommends returning the original RESPONSE CODE (which will typically be 100) with all deposit transactions. Authorization Reversals require the Authorized Amount to be included in the reversal. Action Code for Auth Reversals is L.In the Amount (AMT) field send the amount that was originally authorized. Authorization Reversals are supported for Visa, MasterCard, and MC Diners.

Partical Authorization is supported for American Express, MasterCard, and Visa. You account must be set up to support this

transaction. Action code for Partial Authorization is PA. In a Partial Authorization, the credit card is authorized for the maximum available credit up to and including the requested amount.

If you attempt to authorize $100.00 and the card has only $75 available, the Partial Authorization will succeed, but only for the $75.00.

If you use Partial Authorization, or if you have a division configured to default to Partial Authorization, you must track the Total Authorized Amount (AUTHAMT) response field from Trevance®.This field returns the actual amount that was authorized. There is a new ASIRESP code of 105 indicating a Partial Authorization occurred.

When performing a deposit, refund, or auth reversal, you need to use the value returned in AUTHAMT.

Note that, if you have a division configured to default to Partial Authorization, the Sales transactions sent through the real-time interface will default to Partial Auth, but sales transactions sent through the batch interface will default to Full Auth.

The reason is that Chase Paymentech does not support Partial Auth for Sales (Conditional Deposit) transactions. And Paymentech only supports Auths through the real-time interface. However, when using the Trevance® CN-4250, Trevance® first Authorizes the transaction through the real-time interface (which supports Partial Auth) and, if successful, batches a Deposit transaction for end of day settlement. Trevance® also supports the Full Authorization (FA) action which forces a transaction to fail if the amount requested for authorization is not available. FA must only be used where a division is set up to support Partial Authorizations; otherwise use the standard Authorized (A) action code.

The new (June 2009) Account Check (Y) action code is supported for MasterCard and Visa transactions. Sending an Account Check (Y) with a zero (0) dollar amount verifies the existence of the card. Previously, merchants would typically send a dollar auth that was never deposited. Visa now requires all such transactions to now be Account Checks. MasterCard supports this only for Recurring Billing transactions.

When Trevance® receives an Auth transaction with a zero dollar amount, and the method of payment is either MasterCard or

Visa, it converts that into an Account Check (Y) action. Zero amounts for all other methods of payment are passed directly to Chase Paymentech.

Table 16.4: Chase Paymentech Salem - Purchase Card (Level II)

Authorization	*Auth Reversal*	*Deposit*	*Sale*	*Refund*
Exp Date	Exp Date	Expiration Date	Expiration Date	Exp Date
	Auth Date	Purchase Order Number	Purchase Order Number	
	Auth Code	Tax	Tax	
		Ship To Address (AM)	Ship To Address (AM)	
		Tender Type	Tender Type	
		Authorization Code		
		Authorization Date		

Purchase card (level II) transactions require the same minimum information as a credit card transactions, plus several additional fields.

American Express, MasterCard, and Visa accept level II transactions.

Purchase Card account values can contain spaces or dashes ("-").

You must explicitly identify Purchase Card transactions by importing "P" in the TENDER TYPE field.

You must provide the amount of tax, even if it is $0.00.

Paymentech recommends providing the SHIP TO ADDRESS fields (ADDRESS, CITY, STATE, ZIP) for American Express (AM) purchase card transactions.

Table 16.5: Chase Paymentech Salem - Purchase Card (Level III)

Auth	*Auth Reversals*	*Deposit*	*Sale*	*Refund*
Exp Date	Exp Date	Expiration Date	Expiration Date	Exp Date
	Auth Date	Purchase Order Number	Purchase Order Number	
	Auth Code	Tax	Tax	
		Alternate Tax Amount (MC)	Alternate Tax Amount (MC)	
		Alternate Tax ID (MC)	Alternate Tax ID (MC)	
		Discount	Discount	
		Tender Type	Tender Type	
		Authorization Code		
		Authorization Date		

Purchase card (level III) transactions require the same minimum information as level II transactions, plus several additional fields. Some fields are required only for a specific card type (MC) and are so marked in the chart.

Trevance® supports supplemental records for purchase card (level III) line items. Please see "Appendix B. Level III Transactions" on page 353.

MasterCard and Visa accept level III transactions. You must explicitly identify Purchase Card transactions by importing "P" in the TENDER TYPE field.

American Express provides a similar functionality through the use of four American Express TRANSACTION ADVICE ADDENDUM fields. The field reference list gives details on how these fields are used.

Table 16.6: Chase Paymentech Salem - Third-Party Encrypted Card

Auth	*Auth Reversal*	*Deposit*	*Sale*	*Refund*
Expiration Date	Exp Date	Expiration Date	Expiration Date	Expiration Date
Encrypt Flag	Encrypt Flag	Encryption Flag	Encryption Flag	Encryption Flag
	Auth Code	Authorization Code		
	Auth Date	Authorization Date		

Third-party encrypted credit card account values are a secure way for banks to provide account information to call centers without revealing a customer's credit card account.

A bank provides these numbers, along with customer contact information. The account value is encrypted using a Public/Private Key algorithm. The bank maintains the key for encrypting the account and the processor maintains the key for decrypting only. The merchant is unable to decrypt the account.

Encrypted credit card transactions require the same information as normal credit card transactions with the addition of an ENCRYPTION FLAG. This ENCRYPTION FLAG is provided by Paymentech

and is specific to the bank (or other entity) supplying the account numbers.

Transactions that contain the minimum information plus an ENCRYPTION FLAG are automatically identified as "third-party encrypted credit card" transactions.

The encrypted credit card account value is sent in the ACCOUNT field, just as it is with unencrypted credit card transactions.

Table 16.7: Chase Paymentech Salem - Electronic Checks

Authorization	*Deposit*	*Sale*	*Refund*
Routing Number	Routing Number	Routing Number	Routing Number
BillAddress: First Name	BillAddress: First Name	BillAddress: First Name	Bill Address First Name
BillAddress: Last Name	BillAddress: Last Name	BillAddress: Last Name	Bill Address Last Name

Transactions that contain the minimum information plus a ROUTING NUMBER (also called a bank ID or bank routing number) are automatically identified as electronic checks (eChecks). Trevance® allows you to accept checks electronically (that is, over a secure web interface).

This type of transaction is not designed for handling accounts receivable conversion (ARC) or point of purchase (POP) check conversions. See "Accounts Receivable Check Conversion (ARC)" on page 241 and "Point of Purchase Conversion/Truncation (POP)" on page 242.

Place the checking account number in the ACCOUNT field and the Routing Number (Bank ID or Bank Routing Number) in the ROUTING NUMBER field.

The ACCOUNT field can contain spaces. It must *n*ot have dashes ("-").

Table 16.8: Chase Paymentech Salem - Third-Party Encrypted Electronic Checks

Auth	*Deposit*	*Sale*	*Refund*
Routing Number	Routing Number	Routing Number	Routing Number
Encryption Flag	Encryption Flag	Encryption Flag	Encryption Flag
BillAddress: First Name	BillAddress: First Name	BillAddress: First Name	Bill Address First Name
BillAddress: Last Name	BillAddress: Last Name	BillAddress: Last Name	Bill Address Last Name

Third-party encrypted checking account values are a secure way for banks to provide account information to call centers without revealing a customer's checking account number.

A bank provides these numbers, along with customer contact information. The account value is encrypted using a Public/Private Key algorithm. The bank maintains the key for encrypting the account, and Paymentech maintains the key for decrypting only. The merchant is unable to decrypt the account.

Encrypted check transactions require the same information as normal check transactions with the addition of an ENCRYPTION FLAG. This ENCRYPTION FLAG is provided by Paymentech and is specific to the bank (or other entity) supplying the account numbers.

Transactions that contain the minimum information plus a ROUTING NUMBER and ENCRYPTION FLAG are automatically identified as "encrypted electronic check" transactions.

The encrypted checking account value is sent in the ACCOUNT field, just as it is with unencrypted check transactions.

Table 16.9: Chase Paymentech Salem - Switch/Solo

Authorization	*Deposit*	*Sale*	*Refund*
Expiration Date	Expiration Date	Expiration Date	Expiration Date
Switch/Solo Card Issue Number	Switch/Solo Card Issue Number	Switch/Solo Card Issue Number	Switch/Solo Card Issue Number
Switch/Solo Card Start Date	Switch/Solo Card Start Date	Switch/Solo Card Start Date	Switch/Solo Card Issue Number
	Authorization Code		
	Authorization Date		

Switch and Solo are private label debit cards used in the United Kingdom. Both cards are based in the UK and processed in British Pounds Sterling.

Even though Switch and Solo are debit cards, they are processed very like credit cards.

Switch/Solo transactions are submitted to Paymentech as credit card transactions. Trevance® automatically recognizes Switch/Solo transactions from the `ACCOUNT` value.

If a Switch/Solo card has an issue number, you must provide it. If the card does not have an issue number, you must provide the start date.

Table 16.10: Chase Paymentech Salem - PIN-less Debit

Authorization	*Auth Reversal*	*Deposit*	*Sale*	*Refund*
Expiration Date	Exp Date	Expiration Date		

Continued on next page

Table 16.10 – *Continued from previous page*

Authorization	*Auth Reversal*	*Deposit*	*Sale*	*Refund*
Biller Reference	Biller Reference		N/A	N/A
Tender Type	Tender Type	Tender Type		
		Authorization Code		
		Authorization Date		

PIN-less debit is also known as debit bill payment and is only available to select industries, including utilities, insurance, telecommunications, cable, financial, and government entities. Regulations currently do not allow PIN-less debit to be used for recurring or installment payments.

The PIN-less debit is a single-message transaction. As soon as the transaction is "authorized" money is removed from the customer's account. Paymentech takes the debit authorization data and stores it in a Debit Database. When you send a deposit transaction in the daily batch file, Paymentech matches the deposit against the Debit Database. When a match occurs, money moves to your account. If no match occurs, Paymentech reports the exception to the merchant.

Debit authorization (A) and Sale (S) transactions must occur through the real-time interface.

An exception to the above is that recurring Auth and Sale transactions may be submitted via batch. This requires the Recurring flag to be passed with the transaction. This functionality allows PINless debit cards to be used for recurring payment purposes. The very first transaction still must go through the real-time interface.

Online Deposit and Sale transactions require a Trevance® CN-4250.

Trevance® cannot automatically recognize a PIN-less debit transaction because the fields passed for PIN-less debit are identical to the fields passed for a credit card transaction, and some cards can be used for both credit and debit.

You must include the "L" TENDER TYPE in all PIN-less debit transactions. If you do not provide the TENDER TYPE field, the transaction is processed as a credit card.

Authorization Reversals must be submitted within 90 minutes of the Authorization transaction.

Table 16.11: Chase Paymentech Salem - PIN-based Debit

Authorization	*Auth Reversal*	*Deposit*	*Sale*
Track 1 or Track 2[1]	Account	Account	N/A
PIN	PIN		
KSN [2]	KSN		
Debit Account Type [3]			
Tender Type	Tender Type	Tender Type	
XCLASS[4]			
	Authorization MOP	Authorization MOP	
	Authorization Code	Authorization Code	
	Authorization Date	Authorization Date	

[1]Import either Track 1 or Track 2 data–*not* both. If both tracks are provided, Trevance® uses Track 2 for debit transactions.

[2] The key serial number (KSN) is assigned by Paymentech.

[3] For U.S. debit cards, this field is always blank. For Canadian debit cards, you must ask the customer if this is a Consumer Checking or Consumer Savings account and import a value for this field.

[4] Must be P for Retail (POS).

Table 16.12: Chase Paymentech Salem - PIN-based Debit 2

Refund	*Refund Authorization*	*Refund Auth Reversal*
Account	Track 1 or Track 2[1]	Account
	PIN	
	KSN [2]	
	Debit Account Type [3]	
Tender Type	Tender Type	Tender Type
Authorization MOP		Authorization MOP
Authorization Code		Authorization Code
Authorization Date		Authorization Date

PIN-based debit transactions are retail, card-present transactions.

PIN-based transactions require that the customer swipe their card and also provide their personal identification number (PIN) on a hardware PIN-pad. After the customer enters the PIN, it is encrypted for security purposes. The card-swipe information, the encrypted PIN, and the key serial number (KSN) assigned to the PIN-pad are presented to Trevance®.

Authorization and refund authorization transactions that contain the minimum information plus TRACK 1 or TRACK 2 data,

a PIN, and a KSN are automatically recognized as "PIN-based debit" transactions. You should send only one track, but if both tracks are sent, Trevance® uses TRACK 2 since that is preferred by the payment processor.

Deposit and refund transactions must contain a TENDER TYPE of "D" to identify them as PIN-based debit transactions.

Track data is required for authorization (and reverse authorization) transactions. The account number is required for deposit and refund transactions.

During authorization, Trevance® extracts the account information from the track data and returns it in the ACCOUNT field. Merchants must remember the account number for later submission to Trevance® in a deposit or refund transaction. You must not store track data after the authorization is complete. Trevance® in compliance with Card Association rules, does not export the track data after processing.

PIN-based debit cards require a real-time refund authorization transaction followed by a batch refund settlement transaction. Like the authorization/deposit transactions, both the refund authorization and the refund transactions move money. These transactions must always be issued in pairs and always for the same amount.

The action code for a real-time refund authorization is RA.

Table 16.13: Chase Paymentech Salem - (ARC)

Authorization	*Deposit*	*Sale*	*Refund*
Routing Number	Routing Number	Routing Number	Routing Number
BillAddress: First Name	BillAddress: First Name	BillAddress: First Name	BillAddress: First Name
BillAddress: Last Name	BillAddress: Last Name	BillAddress: Last Name	BillAddress: Last Name

Continued on next page

Table 16.13 – *Continued from previous page*

Authorization	*Deposit*	*Sale*	*Refund*
Check Number	Check Number	Check Number	Check Number
ECP Authorization Method 1	ECP Authorization Method 1	ECP Authorization Method 1	ECP Authorization Method 1
Checking Account Type 2	Checking Account Type 2	Checking Account Type 2	Checking Account Type 2
	Authorization Code		
	Authorization Date		

NOTES:
[1] Although Paymentech allows merchants to set a default value for the ECP Authorization method, Trevance® requires an "A" to be imported as the ECP Authorization Field; the "A" indicates that this is an "accounts receivable check conversion (ARC)" transaction.
[2] If the Checking Account Type field is not provided, Trevance® defaults to Consumer Checking.

Trevance® supports accounts receivable check conversion (ARC) transactions. The merchant is responsible for scanning the paper check and extracting the necessary information to submit to Paymentech through Trevance®.

ARC is designed to improve check handling by turning paper checks into electronic transactions.

Trevance® automatically identifies ARC transactions as "check (tender type K)" transactions.

Table 16.14: Chase Paymentech Salem - POP

Authorization	*Deposit*	*Sale*	*Refund*
Routing Number	Routing Number	Routing Number	Routing Number
BillAddress: First Name	BillAddress: First Name	BillAddress: First Name	BillAddress: First Name
BillAddress: Last Name	BillAddress: Last Name	BillAddress: Last Name	BillAddress: Last Name
Check Number	Check Number	Check Number	Check Number
ECP Authorization Method 1	ECP Authorization Method [1]	ECP Authorization Method [1]	ECP Authorization Method [1]
Checking Account Type [2]	Checking Account Type [2]	Checking Account Type [2]	Checking Account Type [2]
POP Terminal City[3]	POP Terminal City[3]	POP Terminal City[3]	POP Terminal City[3]
POP Terminal State [3]	POP Terminal State[3]	POP Terminal State[3]	POP Terminal State[3]
	Authorization Code		
	Authorization Date		

NOTES:

[1]Although Paymentech allows merchants to set a default value for the ECP Authorization method, Trevance® requires a "P" to be imported as the ECP Authorization Field; the "A" indicates that this is an "point of purchase (POP) check" transaction.

[2]If the Checking Account Type field is not provided, Trevance® defaults to Consumer Checking.

[3]The POP Terminal City and POP Terminal State identify the physical location of the point of purchase activity. Defaults may be set at Paymentech for each division. If a default is set, you do not need to present this field to Trevance®.

Trevance® supports point of purchase (POP) transactions. The merchant is responsible for scanning the paper check and extracting the necessary information to submit to Paymentech through Trevance®.

POP is designed to improve check handling by turning paper checks into electronic transactions at the point of purchase.

Trevance® automatically identifies ARC transactions as "check (tender type K)" transactions.

Table 16.15: Chase Paymentech Salem - Bill Me Later

Authorization	*Deposit*	*Sale*	*Refund*
BML Customer Type	BML Customer Type	BML Customer Type	BML Customer Type
BML Item Category	BML Item Category	BML Item Category	BML Item Category
Product Type		Product Type	
Date of Birth[2]		Date of Birth[2]	
T and C Version[1]	T and C Version	T and C Version[1]	T and C Version
Freight	Freight	Freight	Freight
Customer Registration Date	Customer Registration Date	Customer Registration Date	Customer Registration Date

Continued on next page

Table 16.15 – *Continued from previous page*

Authorization	*Deposit*	*Sale*	*Refund*
Customer Social Security Number[2],[3]	Authorization Code	Customer Social Security Number [2],[3]	
Bill Address: First Name	Authorization Date	Bill Address: First Name	
Bill Address: Last Name		Bill Address: Last Name	
Bill Address: City		Bill Address: City	
Bill Address: State/Province		Bill Address: State/Province	
Bill Address: Zip/Postal Code		Bill Address: Zip/Postal Code	
Bill Address: Country[4]			
Ship Address: Last Name		Ship Address: Last Name	
Ship Address: City		Ship Address: City	
Ship Address: State/Province		Ship Address: State/Province	
Ship Address: Zip/Postal Code		Ship Address: Zip/Postal Code	

BML classifies authorization requests as being of three types:

- Var D: Using dummy account numbers
- Var A1: Real account number stored from previous purchase for existing customer (WEB)
- Var A2: Real account number plus further identifying information (Call Centers)

NOTES:
[1]Var D only
[2]Var D and Var A2 only
[3]Last four digits of social security number only
[4]Must be "US"

Trevance® automatically identifies "Bill Me Later" transactions.

Refer to the on-line field reference list for details on the specific fields.

Chase Paymentech Salem - European Direct Debit

Authorization	*Deposit*	*Sale*	*Refund*
EDD Country Code	EDD Country Code	EDD Country Code	EDD Country Code
EDD Bank Sort Code	EDD Bank Sort Code	EDD Bank Sort Code	EDD Bank Sort Code
EDD RIB Code (optional)	EDD RIB Code (optional)	EDD RIB Code (optional)	EDD RIB Code (optional)
	Bill Address: First Name	Bill Address: First Name	Bill Address: First Name
	Bill Address: Last Name	Bill Address: Last Name	Bill Address: Last Name

The EDD Country Code (EDCNTRY) indicates the country in which the customer's bank is located. It must be one of the

following:

- AT Austria
- BE Belgium
- FR France
- DE Germany
- NL Netherlands
- GB United Kingdom

The EDD Bank Sort Code (EDBSC) identifies the customer's bank. Each country has its own bank sort code format.

The EDD RIB Code (EDRIB) is the bank account checksum. This is optional and used only in France.

Green Dot MoneyPak

Trevance® supports Green Dot MoneyPak through both real-time and batch interfaces

Trevance® supports the following actions:.

Chase Paymentech Salem - Green Dot®MoneyPak

Authorization-A	*Partial Authorization-PA*	*Force Full Auth -FA*	*Deposit-D*
Real-Time/Batch	Real-Time/Batch	Real-Time/Batch	Real-Time/Batch
Account	Account	Account	Account
Amount	Amount	Amount	Amount
Tender Type (M)	Tender Type (M)	Tender Type (M)	Tender Type (M)
			MoneyPak Confirmation ID

Continued on next page

Table 16.17 – *Continued from previous page*

Authorization-A	*Partial Authorization-PA*	*Force Full Auth-FA*	*Deposit-D*
			MoneyPak Transaction ID

Table 16.18:

Balance Inquiry-Q	*Sale-S*	*Refund Auth-RA*	*Refund-R*
Real-Time/Batch	Real-Time/Batch	Real-Time/Batch	Real-Time/Batch[1]
Account	Account	Account	Account
Amount	Amount	Amount	Amount
Tender Type (M)	Tender Type (M)	Tender Type (M)	Tender Type (M)
		MoneyPak Confirmation ID	MoneyPak Confirmation ID
		MoneyPak Transaction ID	MoneyPak Transaction ID

[1] Account and Amount in real-time. All four fields in batch. See refund note in following section

MoneyPak transactions are a two step process requring an authorization followed by a capture action (either Deposit or Refund). Both sales and refunds must be authorized before capture (Auth and Refund Auth).

MoneyPak acts much like a debit card. When the Authorization is performed, money is moved between the card holder's account and the payment processor. When the Deposit or Refund

transaction is performed, the money is moved between the payment processor and the merchant account.

MoneyPak Authorizations (A, PA, FA and RA) return the following MoneyPak-specific fields:

- MoneyPak Confirmation ID (MPCONFID)
- MoneyPak Original Transaction ID (MPORTXID)

MoneyPak transactions do not return Auth Codes. The Auth Code export field is blanks.

Youll also receive the standard Chase Paymentech Response Code; this should be returned in the Deposit (or Refund) transaction.

The two MoneyPak-specific values need to be provided with the Deposit and Refund batch transactions.Alternatively, when Trevance® receives a deposit transaction, it will attempt to look-up this information internally based on the account number, amount, division, order number, and authorization date.

The amount field for a deposit or refund transaction must match the amount that was authorized. This is similar to debit card functionality. Multiple deposits against a single authorization are not available.

The Trevance® CN-4250 is capable of processing Sales (Conditional Deposit) and Refund transactions through the real-time web interface. When a real-time Sale (S or C) transaction is received, Trevance® peforms a real-time authorization which, when successful, is queued for batch deposit later in the day. The AUTHAMT is queued for capture since the merchant's Division may be configured for automatic Partial Authorization.

Since MoneyPak is an over-the-counter pre-paid card, there is no name or address associated with the card. Thus, no AVS. MoneyPak also does not have any card security code value associated with it.

In order to distinguish MoneyPak transactions from credit card transactions, you must send a Tender Type (TENDTYPE) of M.

16.0.17 Important Refund Note

The Refund (R) transaction works slightly differently in the real-time and batch interfaces.

When Trevance® receives a Refund (R) transaction through the real-time interface, it first performs a real-time Refund Authorization (RA) transaction and, on success, queues a Refund (R) batch transaction for end of day settlement.

When Trevance® receives a Refund (R) transaction through the batch interface, it must contain the necessary MoneyPak Confirmation ID and Original Transaction ID fields from a prior Refund Auth transaction

16.0.18 PayPal

Trevance® supports PayPal transasctions through both the real-time and batch interfaces. Note that the Trevance® CN-4250 provides support for real-time transaction types not supported by Chase Paymentech (such as Sale, Capture, and Refund) by converting the real-time request into a queued batch transaction.

Auric appreciates your setting the ButtonSource parameter in your initial call to the PayPal website to: AURIC_CNEXPRESS_ECUS

PayPal transactions require integration with the PayPal website.To support PayPal transactions with Trevance® you first send one of the Set transactions (for example, SA) to Trevance®.Trevance® makes a call to Chase Paymentech which returns a PayPal token on success. Trevance® returns this value in the PYTOKEN field.

Using this token, you redirect the customer to the PayPal site. When the customer has completed authentication, PayPal sens the customer back to your site (to the RTRNURL parameter you send with the initial Set). At this opint, you can use the token value to complete the transaction through Chase Paymentech using Trevance® transactions.

All PayPal transactions must provide the following fields

- AMT (Amount)
- DIVISION
- TENDTYPE (Tender type): Set to: Y

- MRCHORDR (Merchant Order Number)
- ACTION (Action Code)

The following shows:

- Action: an English-language description of the transasction type.
- Trevance® Action: The ACTION sent to Trevance® .
- Required Fields: Fields required to be sent with this transaction, in addition to the standard fields documented above.
- Online and Batch: Chase Paymentech action (or action taken by Trevance® for transactions that are handled locally).

First line names the PayPal Express Checkout action. Second line shows the Chase Paymentech Method of Payment along with Paymentech's Subtype. For example, a notation of ES/A indicates this is Paymentech Action Code ES subtype A.

Table 16.19: Chase Paymentech Salem - PayPal

Action	*Trevance® Action*	*Required Fields*	*Online*	*Batch*
Set for Auth	SA	RTRNURL CNCLURL	Set Express Payment ES/A	
Set for Order	SO	RTRNURL CNCLURL	Set Express Payment ES/O	
Set for Billing Agreement	SC	RTRNURL CNCLURL	Set Express Payment ES/C	
Set for Auth w/ Billing Agreement	SB	RTRNURL CNCLURL	Set Express Payment ES/B	
Set for Order w/ Billing Agreement	SE	RTRNURL CNCLURL	Set Express Payment ES/E	

Continued on next page

Table 16.19 – *Continued from previous page*

Action	*Trevance® Action*	*Required Fields*	*Online*	*Batch*
Get for Auth	GA	PYTOKEN	Get Express Payment EG/A	
Get for Order	GO	PYTOKEN	Get Express Payment EG/O	
Get for Billing Agreement	GC	PYTOKEN	Get Express Payment EG/C	
Get for Auth w/ Billing Agreement	GB	PYTOKEN	Get Express Payment EG/B	
Get for Order w/ Billing Agreement	GE	PYTOKEN	Get Express Payment EG/E	
Auth	A	PYTOKEN PYPAYER	Do Express Payment ED/A	
Auth from Order	A	PYORDR	Do Auth AU/O	Do Auth AU/O
Auth from Contract	A	PYCID	Do Reference AU/B	Do Reference AU/B
Reauth	A	PYTID	Do Re-Auth AU/A	Do Re-Auth AU/A
Auth w/Billing Agreement	AB	PYTOKEN PYPAYER	Do Express Payment ED/B	
Auth from Order with Billing Agreement	AE	PYORDR	Do Auth AU/E	Do Auth AU/E

Continued on next page

Table 16.19 – *Continued from previous page*

Action	*Trevance® Action*	*Required Fields*	*Online*	*Batch*
Sale	S	PYTOKEN PYPAYER	Do Express Payment ED/A Queue to batch on success as Do Capture RG/P	
Sale	S	PYCID		Recurring Sale RG/R
Refund (Memo)	R	CAPDATE PYTID		Memo Post Refund RD/M
Refund	R	PYTID	Queued to Batch	Full Refund RD/F
Partial Refund	PR	PYTID	Queued to Batch	Partial Refund RD/P
Capture	D	PYTID	Queued to Batch	Do Capture RG/P
Capture (Memo)	D	CAPDATE PYTID		Memo Post Sale RG/M
Final Capture	FD	PYTID	Queued to Batch	Do Capture RG/F
Auth Reversal	L	PYTID	Do Void AR/A	Do Void AR/A

Continued on next page

Table 16.19 – *Continued from previous page*

Action	*Trevance® Action*	*Required Fields*	*Online*	*Batch*
Order Reversal	L	PYORDR	Do Void AR/O	Do Void AR/O
Auth Reversal w/ Billing Agreement	LB	PYTID	Do Void AR/B	Do Void AR/B
Order Reversal w/ Billing Agreement	LE	PYORDR	Do Void AR/E	Do Void AR/E
Create Order	OO	PYTOKEN PYPAYER	Do Express Payment ED/O	
Order From Contract	OO	PYCID	Do Reference AU/E	Do Reference AU/E
Create Billing Agreement	OC	PYTOKEN PYPAYER	Do Express Payment ED/C	
Create Order w/ Billing Agreement	OE	PYTOKEN PYPAYER	Do Express Payment ED/E	
Mass Pay PENDING	MP			Mass Pay RG/S
Void	V	PYTID	Remove Previous Sale, Capture, or Refund Transaction from Queued batch. Must be sent prior to batch settlement.	

16.0.19 PayPal Process Flow

The PayPal process flow can be thought of in the following phases:

- Initiation
- Authentication
- Authorization
- Capture

Initiation, Authorization, and Capture occur through the Trevance® interface to Chase Paymentech. Authentication occurs on the web through interaction with the PayPal site.

A typical sale transaction would be as follows:

- SA (Set for Auth): Get back a PYTOKEN
- Redirect to PayPal web site for authentication. Use the PYTOKEN value as the PayPal Token parameter.
- GA (Get for Auth): Get customer information (name, shipping address, etc.) as well as PYPAYER.
- Auth (Authorise): Get back a PYTID.
- D (Capture): Capture the authorization using the PYTID returned by the Auth. Get back a different PYTID which refers to the capture itself.

You can also work with Orders, which allow multiple authentication:

- SO: Set for Order. Get back a PYTOKEN.
- Redirect to PayPal web site for authentication. Use the PYTOKEN value as the PayPal Token parameter.
- GO (Get for Order): Get customer information (name, shipping address, etc.) as well as PYPAYER.
- OO (Create Order): Get back a PYORDR value.
- A (Authorise from Order): Get back a PYTID.
- D (Capture): Capture the authorization using the PYTID returned by the Auth. Get back a different PYTID which refers to the capture itself.

You can create contracts:

- SC: Set for Contract. Get back a PYTOKEN.

- Redirect to PayPal web site for authentication. Use the PYTOKEN value as the PayPal Token parameter.
- GC (Get for Contract): Get customer information (name, shipping address, etc.) as well as PYPAYER.
- OC (Create Billing Agreement): Get back a PYCID value.
- A (Authorise from Contract): Get back a PYTID.
- D (Capture): Capture the authorization using the PYTID returned by the Auth. Get back a different PYTID which refers to the capture itself.

  You could also create an order from contract and then auth/capture against that.

In order to simplify recurring billing, Chase Paymentech has a Recurring Sale transaction which is available only in Batch mode. Trevance® implements this Recurring Sale as an S transaction.

Note that the S transaction for the real-time/web works differently from the S transaction for batch.

When doing refunds, the PYTID returned from the Capture must be used. Note that this PYTID is only returned from the batch interface, not the web interface as Paymentech does not support real-time capture.

Get returns customer information in the usual fields you would send to Paymentech for a credit card or check transaction: BILLFNAM, BILLLNAMe, BILLEMAL, etc.)

Table 16.20: Chase Paymentech Salem - Retail Credit Card Swipe

Authorization	*Deposit*	*Sale*	*Refund*
Track 1 or Track 2	Account	Track 1 or Track 2	Account
	Expiration Date		Expiration Date

Continued on next page

Table 16.20 – *Continued from previous page*

Authorization	*Deposit*	*Sale*	*Refund*
	Authorization Date		
	Authorization Code		

Trevance® automatically recognizes "retail credit card swipe" transactions.

Either TRACK1 or TRACK 2 data can be provided. If both are provided, Trevance® uses TRACK 1 since it contains more data.

During authorization, Trevance® extracts the account and expiration date from the track data and returns it in the ACCOUNT and EXPIRATION fields. Merchants must remember this data for later submission to Trevance® in a deposit or refund transaction. You must not store track data after the authorization is complete. Trevance® in compliance with Card

Table 16.21: Chase Paymentech Salem - Retail Credit Card Manually Entered

Authorization	*Deposit*	*Sale*	*Refund*
Expiration Date	Expiration Date	Expiration Date	Expiration Date
Zip Code	Zip Code	Zip Code	Zip Code
Class	Class	Class	Class
	Authorization Date		

Continued on next page

Table 16.21 – *Continued from previous page*

Authorization	*Deposit*	*Sale*	*Refund*
	Authorization Code		

Manually entered retail credit card transactions look very much like card-not-present credit card transactions.

You must provide the minimum information plus the card's EXPIRATION DATE and ZIP CODE (postal code).

Manually entered retail credit card transactions must import a "P" in the TRANSACTION CLASS field.

16.0.20 Revolution Money/Revolution Card

Trevance® supports Revolution Card in both Card Present (retail) and Card Not Present environments. The mandatory fields needed to support these transactions are listed in the two tables below.

Revolution Card processes much like a Debit Card. There is an initial authorization, followed by a deposit transaction. The amount you deposit must match the amount you authorize. If you do not deposit, you must reverse the authorization. Similarly, you must perform a realtime refund auth followed by a batch refund. If necessary, you can reverse a Refund Authorization using the RL action.

Revolution Card supports both a Full and Partial Authorization. In Full Authorization mode, the transaction will decline if the full amount requested cannot be obtained. In Partial Authoriation mode, the transaction will succeed if any amount can be obtained from the card. The amount obtained is returned in the AUTHAMT (Authorized Amount) field. When selecting to do simple Authorization, the transaction will operate based on the Full/Partial setting configured for your division at Chase Paymentech.

The XCLASS field must be sent with each transaction (or you can specify a default XCLASS when configuring imported fields).

For Card Present transactions, the XCLASS is P for POS/retail. For Card Not Present, XCLASS may be set to E (Ecommerce), M (Mail Order/ Phone Order), R (Recurring), I (Installment), or D (Chase Paymentech Default). If you specify an XCLASS of "D", Trevance® sends a blank transaction type to Chase Paymentech and the transaction type assumes the default value for the Division.

Notes

- CN-4200 supports only real-time authorizations (both auth and refund auth). Follow-up Deposit and Refund transactions must be sent via batch.
- When CN-4250 receives a real-time Sale transaction, it does a real-time Auth and, if successful, queues a batch Deposit for later automatic settlement. When CN-4250 receives a real-time Refund (R) transaction, it automatically performs a refund auth and queues a batch refund for later settlement. If you want to submit a refund authorization only (which you must later settle with a batch request), specify RA, rather than R, as the Action.
- Sales and Refund transactions may be sent via batches. For card present transactions, you must have obtained a refund authorization on-line (by submitting an R or RA to CN-4200 or RA to CN-4250, as described above) before you can successfully submit a batch refund request. Card not present refunds do not require refund authorization.

Table 16.22: Chase Paymentech Salem - Card Not Present

Action	*Required Fields*	*Online*	*Batch*

Continued on next page

Table 16.22 – *Continued from previous page*

Action	*Required Fields*	*Online*	*Batch*
A: Authorization	ACCT AMT XCLASS TENDTYPE TOKEN	Y	Y
PA: Partial Authorization	ACCT AMT TENDTYPE XCLASS TOKEN	Y	Y
FA: Full Authorization	ACCT AMT TENDTYPE XCLASS TOKEN	Y	Y
S/C: Sale	ACCT AMT TENDTYPE XCLASS TOKEN	Y	Y
D: Deposit	ACCT AMT TENDTYPE AUTHCODE MRCHORDR	CN-4250	Y
L: Auth Reversal	ACCT AMT TENDTYPE AUTHCODE MRCHORDR	Y	Y

Continued on next page

Table 16.22 – *Continued from previous page*

Action	*Required Fields*	*Online*	*Batch*
Y	ACCT AMT TENDTYPE XCLASS SHIPZCPC	Y	Y

Table 16.23: Chase Paymentech Salem - Card Present Transactions

Action	*Required Fields*	*Online*	*Batch*
A: Authorization	TENDTYPE TRACK2 PIN KSN CNACTION AMT XCLASS	Y	N
PA: Partial Authorization	TENDTYPE TRACK2 PIN KSN CNACTION AMT XCLASS	Y	N

Continued on next page

Table 16.23 – *Continued from previous page*

Action	*Required Fields*	*Online*	*Batch*
FA: Full Authorization	TENDTYPE TRACK2 PIN KSN CNACTION AMT XCLASS	Y	N
S/C: Sale	TENDTYPE TRACK2 PIN KSN CNACTION AMT XCLASS	CN-4250	Y
RA: Refund Authorization	ACCT TENDTYPE TRACK2 PIN KSN CNACTION AMT XCLASS	Y	N
D: Deposit	ACCT TENDTYPE AUTHCODE MERCHORDR AMT	CN-4250	Y

Continued on next page

Table 16.23 – *Continued from previous page*

Action	*Required Fields*	*Online*	*Batch*
R: Refund	ACCT TENDTYPE AUTHCODE MERCHORDR AMT	CN-4250	Y
L: Auth Reversal	ACCT TENDTYPE AUTHCODE MERCHORDR AMT	Y	N
RL: Refund Auth Reversal	ACCT TENDTYPE AUTHCODE MERCHORDR AMT	Y	N

16.1 Gift Cards

Trevance® supports Chase Paymentech gift cards. All gift card functionality is available in real-time in both the Trevance® CN-4200 and the CN-4250 and in batch in the CN-3500, CN-4200, and CN-4250. Chase Paymentech supports all gift card actions in both real-time and through batch. In real-time, all transactions are passed directly through to Chase Paymentech, unlike credit cards which have only real-time authorization support on the Chase Paymentech Salem platform.

Trevance® always sends Gift Card transactions marked as Retail (RE).

Gift cards currently support only US Dollars.

16.1.1 Gift Card Specific Fields

Gift Card functionality introduces a new field:

GCORTXID A/N[40] Gift Card Original Transaction ID

The GCORTXID field is returned by for online authorization transactions. This field is used to identify the authorization for subsequent reversal transactions. Merchants should track this number in order to support reversals.

Note: Trevance® can track the GCORTIX and it can be looked up based on the account number, amount, division, order number, and authorization date fields; but it is best practice for the merchant to track this number with the order.

The ability to process gift card sales is tied to the Users's 'R' privilege (Refund and Gift Cards). This privilege is not assigned by default to new users.

The Gift Card Tender Type is 'G'

16.1.2 Gift Card Action Codes

The following action codes are applicable to Gift Cards:

Table 16.24: Gift Card Actions

Trevance® Action Code	**Paymentech Action Code**	**Description**
IS	SI	Issue Account
IR	IR	Issue Account Reversal
CL	SD	Deactivate/Close Account
CR	DV	Deactivate/Close Account Reversal

Table 16.24 – continued from previous page

Trevance® Action Code	**Paymentech Action Code**	**Description**
AO	SV	Reactivate Account
AR	AV	Reactivate Account Reversal
HA	BA	Activate Block (Batch)
HR	BV	Activate Batch (Batch) Reversal
AV	SA	Add Value
RV	VR	Add Value Reversal
BA	BI	Balance Inquiry
S	RP	Redemption/Sale
VS	PV	Redemption/Sale Reversal/Void Sale
A	AU	Authorization
L	AR	Authorization Reversal
D	RC	Redemption Completion
V	CV	Redemption Completion Reversal/Void
D	DP	Deposit

Table 16.24 – continued from previous page

Trevance®	**Paymentech**	**Description**
Action	**Action**	
Code	**Code**	
R	RF	Refund
VR	RV	Refund Reversal

16.1.2.1 Required Fields

All Gift Card transactions require the following fields:

- ACTION
- DIVISION
- XCLASS
- MRCHORDR
- ACCT
- TENDTYPE (set to G)

All transactions except the Balance Inquiry (BA) require the Amount (AMT) field as well. Balance Inquiry returns the current account balance in the CURBAL field.

16.1.2.2 Issue Account: IS

Issue and activate a gift card account with a beginning value.

- On-line and batch.
- Amount field is value to put on card (cannot be 0).

16.1.2.3 Issue Account Reversal: IR

Reverse a prior issue account transaction.

- On-line only.

16.1.2.4 Deactivate/Close Account: CL

Set gift card account to inactive state.

- On-line only.
- TODO: Does CURBAL contain the previous balance?

16.1.2.5 Deactivate/Close Account Reversal: CR

Reverse a prior deactivate transaction.

- On-line only.
- Amount must be previous balance returned by the deactivate transaction.

16.1.2.6 Reactivate Account: AO

Reactivate a gift card account that was previously deactivated.

- On-line only.
- Amount field is value to put on card.

16.1.2.7 Reactivate Account Reversal: AR

Reverse a prior reactivate account transaction.

- On-line only.

16.1.2.8 Activate Block (Batch): HA

Activate a block of up to 100 gift card accounts at one time.

- On-line only.
- Account number is first account number in the block.
- Amount is the value to put into all accounts.
- Number of accounts to activate is sent in the Block Size (BLOCKSZ) field.

16.1.2.9 Activate Block (Batch) Reversal: HR

Reverse a prior block activation transaction.

- On-line only.
- Amount is value used in the original block activation transaction.
- Account number is the first account number in the block.
- Number of accounts to deactivate is sent in the Block Size (BLOCKSZ) field.
- Original Transaction ID (GCORTXID)

16.1.2.10 Add Value: AV

Add amount to value of an active give card.

- On-line and batch.

16.1.2.11 Add Value Reversal: RV

Reverse a prior add value transaction.

- On-line only.

16.1.2.12 Balance Inquiry: BA

Obtain the current balance on a gift card account.

- On-line and Batch.
- Balance returned in the Current Balance field (CURBAL).

16.1.2.13 Redemption/Sale: S

Check the available balance on the gift card account and, if the balance is sufficient, redeems the amount from the account.

- On-line only.

16.1.2.14 Redemption/Sale Reversal/Void: L

Reverses a prior redemption transaction.

- On-line only.
- Original Transaction ID (GCORTXID)

16.1.2.15 Authorization: A

Verifies sufficient funds are available on the account and reserves the requested amount. Amount is reserved on account until action code D (Redemption Complete in real-time and Deposit in batch) or L (Authorization Reversal).

- On-line and Batch.

Note: Authorizations work differently for one specific Merchant Category Code (MCC). If an authorization is sent for merchants with an MCC of 5542, and the authorization amount is $1.00, the entire balance of the card is locked. Otherwise, only the requested amount is locked. For merchants with an MCC of 5542, authorization expires in three hours. Otherwise, authorizations are good for 7 days.

MCC is typically set per division at Chase Paymentech. It can also be defaulted in the Trevance® console or sent with each transaction.

16.1.2.16 Authorization Reversal: L

Reverse a prior authorization and remove the amount lock from the account. Authorization reversal is only valid if the authorization has not expired.

- On-line and Batch.
- Requires original authorization code and authorization date.

16.1.2.17 Redemption Completion: D

Redeem the amount locked in a prior authorization. This is similar to a deposit transaction for a credit card. Redemption amount must be the same as the amount previously authorized. Trevance® uses the same action code (D) for both real-time and batch even though Chase Paymentech uses two different action codes.

- On-line only.
- Requires original authorization code and authorization date.

16.1.2.18 Redemption Completion Reversal/Void: V

Reverse a prior redemption completion transaction.

- On-line only.
- Original Transaction ID (GCORTXID)

16.1.2.19 Deposit: D

Redeem the amount processed in a prior authorization. This is similar to the on-line, real-time Redemption Completion. Redemption amount must be the same as the amount previously authorized. Note that Deposit is batch only and Redemption Completion is real-time only. Trevance® uses the same action code (D) for both real-time and batch even though Chase Paymentech uses two different action codes.

- Batch only.
- Requires original authorization code and authorization date.

16.1.2.20 Refund: R

Add amount to the balance of an active gift card account.

- On-line and Batch.

16.1.2.21 Refund Reversal: VR

Reverse a prior refund transaction.

- On-line only.
- Original Transaction ID (GCORTXID)

16.2 Account Updater

Trevance® has always supported the ability to download Chase Paymentech Account Updater electronic reports. As of Trevance® Version 2.2.15, you can also request updates dynamically via the Batch interface.

Account Updater transactions may only be submitted via the batch import interface. Transactions with a response code of 100

are successfully accepted for account update report. The report is downloaded separately as an electronic report or DFR.

16.2.1 Account Updater Action Codes

The following action code is applicable to Account Updater:

Table 16.25: Account Updater Action Codes

Trevance®	**Paymentech**	**Description**
Action	**Action**	
Code	**Code**	
UP	UP	Account Updater Request

16.2.1.1 Required Fields

All Account Updater transactions require the following fields:

- ACTION
- DIVISION
- ACCT

Trevance® will also send the method of payment and an amount of 0.00 in the upload. Since only MasterCard and Visa cardholder accounts are acceptable in Account Updater transactions, Trevance® automatically recognizes what the card type is and transmits it to Chase Paymentech.

16.3 Fraud Scoring

Trevance® supports the Chase Paymentech Safetech Fraud Scoring capability (also known as Kount) for real-time E-commerce

transactions with credit cards, checks, and PayPal. This service allows merchants to configure their own fraud rules and to determine when fraud checks will occur. When implementing this service, you will need to add some Kount-specific code to your web site. Please refer to your Chase Paymentech Safetech Fraud documentation for details.

16.3.1 Additional Fields

Once the Fraud functionality is activated for your account, using it requires sending just a few additional fields. Either:

- Set a Fraud ID for the Division in the Trevance® Console (will activate Fraud checking for all transactions).
- Send a Fraud ID in the real-time transaction (allows you to decide when to check fraud on a transaction-by-transaction basis.

In addition to this simple step, there are additional fields you can send that help the Safetech Fraud Scoring system evaluate a transaction:

Table 16.26: Optional Fields for Safetech Fraud

Trevance® Field	**Description**
CUSTGNDR	Customer Gender (M or F)
CUSTID	Customer Identifier. A unique identifier from your organization to track multiple transactions from the same customer.
CUSTIDDT	Date and time the CUSTID was created.
CUSTIP	Internet address of customer during an E-commerce transaction.

Table 16.26 – continued from previous page

Trevance® Field	Description
CUSTSID	Merchant-generated session ID for the customer.
FENCAMT	Fencible amount. Cash value of fencible items in order.

In addition to the fields cited above, you should also send the billing and shipping address as well as any billing and shipping email addresses and phone numbers that are associated with the transaction.

16.3.2 Fraud Responses

Fraud responses are returned separately from the processing response code.

Table 16.27: Safetech Fraud Response Fields

Trevance® Field	Description
CUSTPRXY	Y if customer connected through a proxy. Otherwise N.
CUSTTZ	Customer's timezone. Offset in minutes from UTC.
FRAUD14D	Fraud 14 day velocity.
FRAUD6HR	Fraud six hour velocity.

Table 16.27 – continued from previous page

Trevance® Field	Description
FRAUDXID	Fraud assessment ID. Unique identifier for this fraud assessment.
FRAUDADR	Fraud auto decision response.

Value	Description
A	Approve
D	Decline
M	Manager Review
R	Review

FRAUDBRC	Customer's browser's country setting.
FRAUDBRL	Customer's browser's language setting.
FRAUDCXT	Number of transactions associated with card.
FRAUDCK	Y if customer's browser allows cookies. Otherwise N.
FRAUDDVC	Fraud device (browser) country. Country associated with device.
FRAUDDVT	Fraud device (browser) local date and time.

Table 16.27 – continued from previous page

Trevance® Field	Description
FRAUDDVF	Fraud device fingerprint. A 32-character hash of system identifiers considered to be constants on a device (browser).
FRAUDDVL	Fraud device layers. Five 10-character description values, delimited by periods, that identify device properties or characteristics at the network, Flash, JavaScript, HTTP, and browser layers.
FRAUDDVR	Fraud device region. Region associated with device.
FRAUDDXT	Fraud device transactions. Number of transactions associated with this device.
FRAUDEXT	Fraud email transactions. Number of transactions associated with this email.
FRAUDFL	Y if customer browser allows Flash. Otherwise N.
FRAUDJS	Y if customer browser allows JavaScript. Otherwise N.
FRAUDKMF	Fraud Kaptcha Match Flag. Y if an RIS has a corresponding Kaptcha record. Otherwise N.
FRAUDMD	Y if transaction is from a mobile device. Otherwise N.
FRAUDMDT	Fraud mobile device type. A descriptive text of the device.
FRAUDMW	Y if device is wireless.

Table 16.27 – continued from previous page

Trevance® Field	Description
FRAUDNWT	Single-character describing the type of network used.

Value	Description
A	Anonymous
H	High School
L	Library
N	Normal
P	Prison
S	Satellite

FRAUDPYB	Payment brand identified during fraud scoring.
FRAUDRGN	Fraud region associated with customer. If region is uppercase, it represents a country (e.g., CA for Canada). If region is lowercase, it represents a state or province (e.g., ca for California).
FRAUDRPC	Y if device is a remotely controlled computer. Otherwise N. Return
FRAUDSCR	Fraud risk score. A two-digit number. See your Chase Paymentech documentation for details on how to interpret the score.

Table 16.27 – continued from previous page

Trevance® Field	**Description**
FRAUDST	Fraud status code. A four-character value. See your Chase Paymentech documentation for details on how to interpret the fraud status code.
FRAUDVD	Y if the device is voice controlled. Otherwise N.
FRAUDCTR	Worst country associated with customer in last 14 days. Return value uses the ISO 3166 alpha code.

16.3.3 ValueLink

Trevance® CN-4250 provides custom support for the ValueLink processing service. This functionality is available only via custom request. Please call Auric Systems International for more information.

ValueLink is supported exclusively through the real-time Web interface. All ValueLink functionality is supported via Chase Paymentech's Direct On-Line specification.

The fields required for each ValueLink action are as follows:

Table 16.28: Chase Paymentech Salem - ValueLink Fields

Sale (S)	*Balance Inquiry (Q)*
Account	Account

Continued on next page

Table 16.28 – *Continued from previous page*

Sale (S)	*Balance Inquiry (Q)*
Amount	
Division ID	Division ID
Merchant Order Number	
TenderType (V)	TenderType (V)
Class (E)	Class (E)

The Paymentech Method Of Payment (MOP) value is determined in Trevance® by a combination of Card Type and Tender Type. For ValueLink, Leave Card Type Blank (or do not send it) and set Tender Type to V.

ValueLink supports the following actions:

- Q Balance Inquiry
- S Sale

ValueLink supports conditional deposit (one-transaction auth and capture–or auth and auth-completion).

On a Balance Inquiry transaction, the account balance is returned by Trevance® in the Current Balance (CURBAL) field. You must include this field in the set of Web Export response fields when using Balance Inquiry.

Note that Amount is required to be sent on a Balance Inquiry transaction. Trevance® requires the Amount field in all transactions. For Balance Inquiry, the Amount field is ignored and not sent to Paymentech. It can be set to 0.

Notes:

- CVV and AVS not supported

- ValueLink cards are 16 digits and start with 6. They do meet
  LUHN-10.
- Chase Paymentech supports duplicate detection on ValueLink sales transactions. Duplicate parameters are the order #, Account #, Division Number and Amount of Authorization. There is no duplicate detection on ValueLink Sales transactions. A merchant must check with ValueLink's Support Desk if no response is received. Chase Paymentech would submit a duplicate Sale if the transaction were submitted by the merchant after having not received a response from Chase Paymentech.

16.3.3.1 Response Reason Codes

Following standard Paymentech codes are returned by ValueLink transactions.

PTI Code PTI Description
100 Successfully Approved
302 Insufficient funds
754 Account has been closed
825 Account does not exist
806 Card has been restricted
522 Card has expired
833 Division Number is Incorrect
902 System error/malfunction with issuer
502 Card reported as lost/stolen
303 Generic decline - No other information is being provided
225 Data within transaction is incorrect (D)
243 Data is inaccurate or missing (D)
521 Insufficient funds/over credit limit
607 Amount not accepted by ValueLink
227 Specific and relevant data within transaction is absent (D)
510 Exceeds withdrawal or activity count limit
253 Invalid transaction type for order (D)
758 Transaction posting to account prohibited
594 Unidentifiable error. ValueLink Generated

204 Unidentifiable Error
301 Authorization network couldn't reach ValueLink

16.4 Card-Type Indicator

Trevance® supports the Paymentech Card-Type Indicator for real-time and batch transactions for certain card types. To use this feature in Trevance®, set the RQCRDINF field to "Y" on either an online or batch transaction. Detailed card type information will then be returned in these fields:

CARDCTRY	The country of the issuing bank
CARDATTR	Additional attributes pertaining to the card.

CARDATTR responses may be zero or more of the following strings, separated by spaces if more than one is applicable:

ISSREG	Issuer regulated under Durbin
ISSUNREG	Issuer unregulated under Durbin
PCL2	Purchase card level 2 support
PREPAID	Prepaid card
PAYROLL	Payroll card
HEALTHCARE	Healthcare card
AFFLUENT	Cardholders with higher limits
SIGDEBIT	Signature debit card
PINLESS	Pinless debit card
PCL3	Purchase card level 3 support

Detailed card information is supported for auth/sale, query, and verify actions for the following card types:

- Visa
- Mastercard
- Discover
- JCB

17 Chase Paymentech Solutions PNS/Tampa

Trevance® CN-4250 provides custom support for Disney Rewards Card via the Chase Paymentech Solutions PNS (Tampa) platform. All Disney Rewards Card functionality is provided through the CN-4250 real-time Web interface. There is no batch interface to the Rewards functionality.

Support for Chase Paymentech Solutions PNS is provided on a custom basis. Please contact Auric Systems International for additional information on this capability.

Trevance® CN-4250 communicates with Paymentech PNS via VPN or Frame Relay. Both VPN and Frame Relay provide highly reliable communication and rapid transaction turn-around times. Paymentech states that real-time transactions reliably process in 3 to 4 seconds. Trevance® provides a built-in failover mechanism. Paymentech can provide merchants with additional redundant failover configurations. Please contact your Paymentech representative for details.

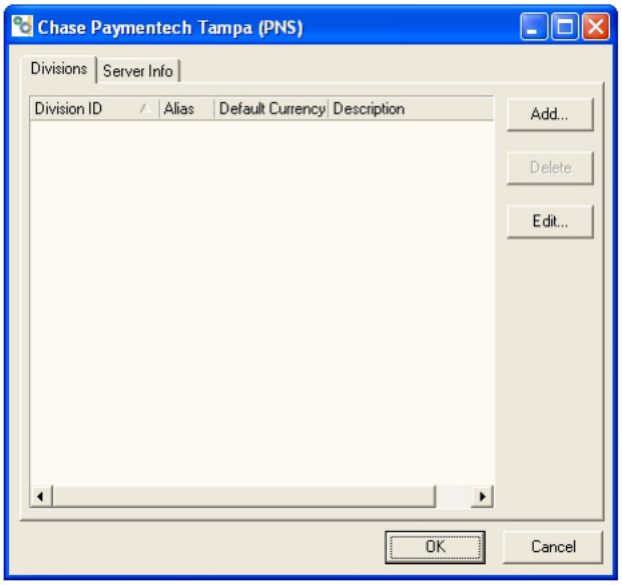
Trevance® currently supports only the Paymentech PNS On-Line (realtime) service. It implements the PNS ISO Formats in Host Capture mode. When setting up with Paymentech PNS, please request them to select Host Capture and to allow up to 10 simultaneous asynchronous transactions.

Please refer to the Trevance® README file to determine the latest Paymentech specification to which Trevance® has been certified.

Configuring Processor Settings

To configure the processor settings:

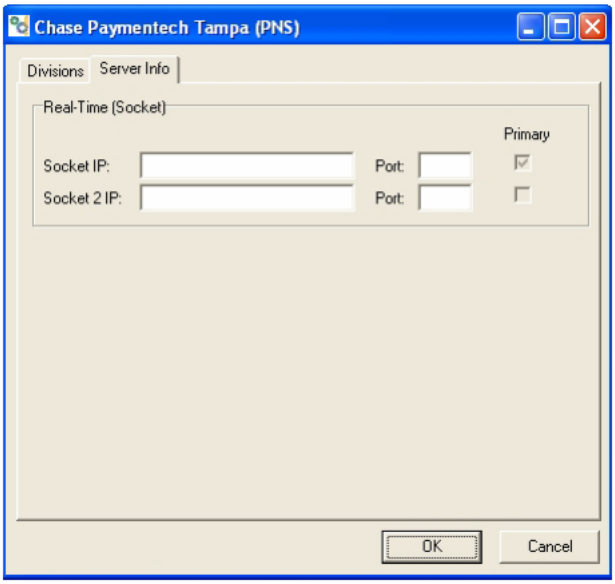
1. Click on CONFIGURE.
2. If the server isn't paused, click on *PAUSE SERVER TO CONFIGURE ITEMS BELOW*.
3. Click on Processor Settings to view a screen like the following:



The screen, tabs, and boxes that you see are set up specifically for Paymentech PNS. Paymentech provides you with the settings required to complete this configuration.

17.0.1 Server Info

1. Click on the SERVER INFO tab.



SERVER INFO allows you to configure up to two socket connections to PNS. The first connection is your primary connection. The second (optional) connection is your failover in case there should be communications problems with your primary connection.

Secondary (or failover) connections are not required.

2. Fill in the SOCKET IP (Paymentech will provide this in IP notation such as: 10.20.33.129). Fill in the SOCKET PORT. Paymentech provides this specific information in a settings document.
3. If you are using secondary (failover) connection, enter the SOCKET2 IP and SOCKET2 PORT information.

17.0.2 How Failover Works

The Trevance® failover mechanism works as follows:

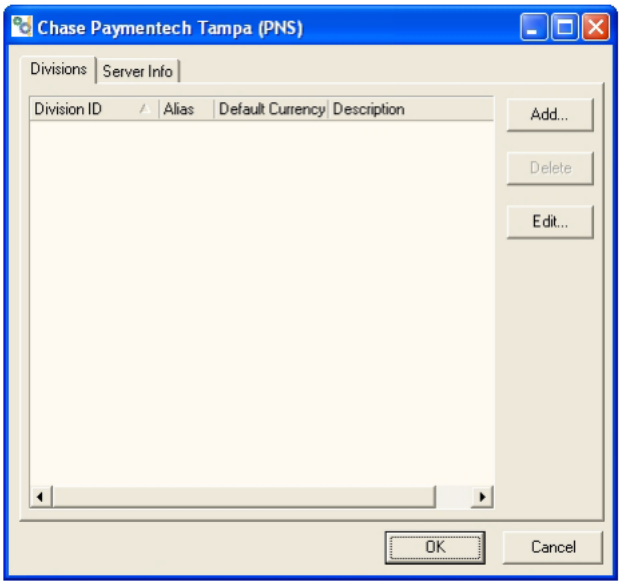
- When two Socket IP connections are defined, Trevance® uses one as the Primary and one as the Secondary.
- The Primary Connection is indicated by a checkmark in the Server Configuration screen (see above).
- All real-time transactions are sent to the Primary Connection.
- If the Primary Connection is unavailable (disconnected), Trevance® switches to sending transactions to the Secondary Connection.
- If a real-time transaction is sent and never received because the socket disconnects, Trevance® eventually times-out the transaction and returns with a timeout error. Trevance® **does not** automatically retransmit the transaction. The decision to retransmit a real-time transaction is left as a business decision on the merchant side. Retransmitting some transactions (such as debit card authorizations) have monetary consequences.
- If a transaction timeout is received, Trevance® switches connections.

- Primary socket connection can also be set manually without pausing Trevance® . Select Server/Primary Real-Time Socket from the menu and select which socket you want to use as the Primary socket.

- A log entry appears whenever connections are switched.

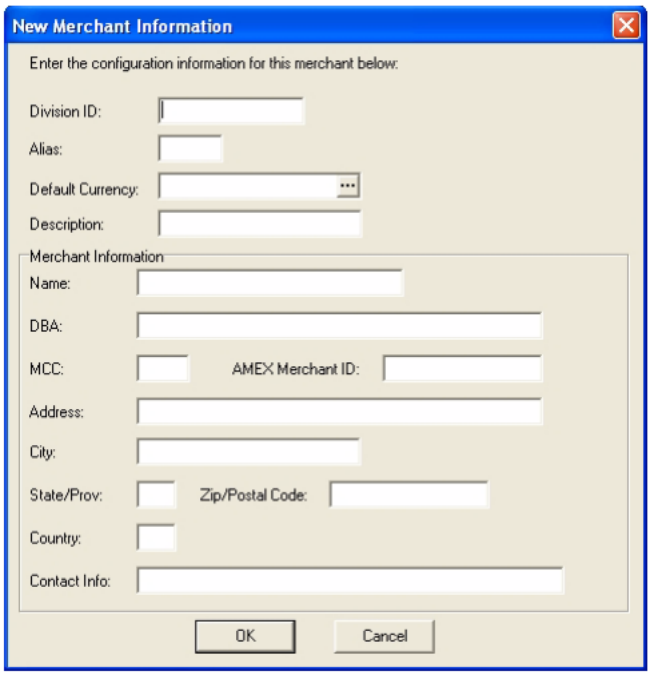
17.0.3 Divisions

1. Click on the DIVISION tab to view a screen like the following:



Merchant IDs are used to identify transactions sent for different categories, such as the different parts of a large company, mail order/phone order/web sales, or totally different companies (as in the case of an in-bound call center processing for many merchants).

To add a division:



2. Click on

3. Enter your MERCHANT ID. This 12-digit number is supplied by Paymentech and must be typed exactly as supplied.

4. The ALIAS field is provided for future functionality. Leave it blank for now.

5. Under Default Currency, click on to view a list of currencies. Currently, The Trevance® /PNS functionality supports only US currency. Leave blank for the default value.

6. Enter a DESCRIPTION. This information appears only in the Trevance® UI and provides a hint to you as to the use of each MERCHANT ID. This information is never sent to Paymentech.

7. Enter the appropriate MERCHANT INFORMATION. Note: None of the MERCHANT INFORMATION is required when using Disney Rewards Cards. This information provided for future expansion to other payment methods such as credit cards, checks, etc.

8. Name is your company name.

9. If you have a DBA ("Doing Business As", tradename, corporate division, etc.) enter it here.

10. MCC and AMEX Merchant ID are specific to MasterCard and American Express transactions. Since only Disney Rewards cards are currently supported, these fields will be blank.

11. Enter your Business street address, City, State/Prov, and Zip/Postal Code.

12. Enter your Country code. Currently only US is supported.

13. Enter your contact information. This is typically the customer contact 1.800 number.

14. Click on

17.1 Configuring Transaction Defaults

This section covers Paymentech PNS-specific details of real-time web configuration.

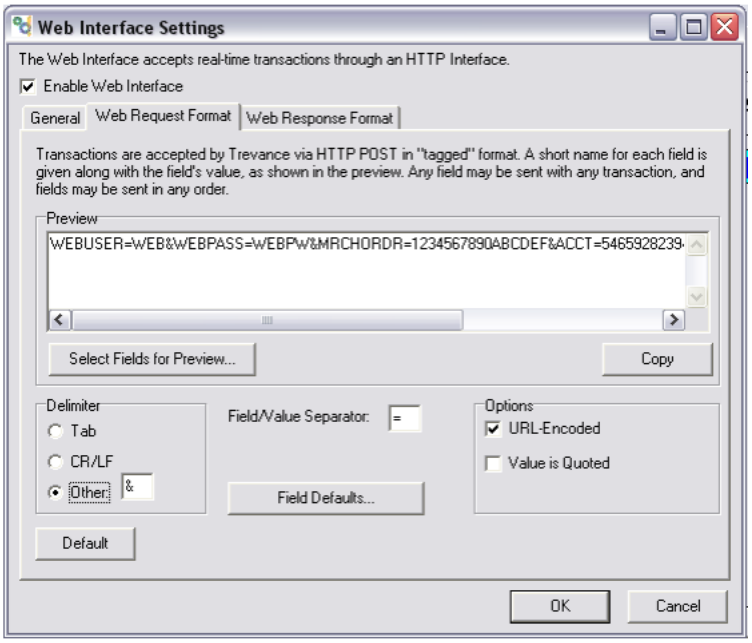
17.1.1 Configure Web Transaction Defaults

Refer to "Configuring the Real-Time Web Interface" on page 80 for general information on web transaction configuration.

1. Click on CONFIGURE.

2. If the server isn't paused, click on *PAUSE SERVER TO CONFIGURE ITEMS BELOW*.

3. Click on REAL TIME WEB INTERFACE, then the WEB REQUEST FORMAT tab to view the Web Transaction form:



4. Click on to view:

This screen lets you select default information for Trevance® to use with the transaction if certain fields are missing.

- ACTION: Select S: Conditional Deposit. Auric recommends always sending a valid ACTION field in your transactions.
- DIVISION ID: This is the Paymentech division ID that is assumed for all transactions submitted with a division. If you are processing a single Division, then it is suitable to use the Default. If are using multiple (or expect to be using multiple divisions in the future) then leave this blank and always send a DIVISION ID with each transaction.
- CLASS: Many merchants have Paymentech assign a specific transaction class to each division. Select MERCHANT DEFAULT to use the Paymentech configuration.
- PRODUCT DELIVERY TYPE: Select if you are sending Physical or Digital goods.

- ECOMMERCE: This field describes the method by which ecommerce transactions are received. The most common is ENCRYPTED (HTTPS), indicating a secure web transaction.

17.2 Methods of Payment, Actions, and Required Fields

Trevance® for Paymentech PNS supports the following methods of payment (MOPs):

- Disney Rewards Cards

17.2.1 Required Information

Regardless of the method of payment, Paymentech transactions require the following information:

- ACCOUNT: Credit card, debit card, or bank account number.
- ACTION: Authorization, sale, deposit, refund. Set to default or import with each transaction.
- AMOUNT
- DIVISION ID: Set to default or import with each transaction.
- MERCHANT ORDER NUMBER: Every transaction requires a merchant order number. This value is used for tracking transactions through Paymentech and the Card Associations.
- Merchants should provide a MERCHANT ORDER NUMBER with each transaction. Trevance® generates an order number if one is not provided. If you're performing two-pass authorization transactions that are followed by deposits, you must use the same order number for the deposit *and* for the authorization. A unique order number for each transaction helps reporting and reconciliation, but is not mandatory for Paymentech.

17.2.2 Supported Disney Rewards Cards Actions

Trevance® supports the following actions for the Disney Rewards Card:

- Authorize (A): Obtain an authorization for the requested amount, if available. If not available approval may be given for a lower amount. In either case, the actual authorized amount is returned in the Authorized Amount (AUTHAMT) field.
- Deposit (D): Capture funds from a previous authorization. Include the actual Authorized Amount (AUTHAMT) from the initial Authorize transaction.
- Refund (R): Return funds to the customer account.
- Sale (S): Obtain an authorization for the requested amount, if available. If not available approval may be given for a lower amount. In either case, the actual authorized amount is returned in the Authorized Amount (AUTHAMT) field. If the transaction succeeds, it is automtically captured by Chase Paymentech for later settlement. i.e., no need for a separate Deposit.
- Balance Inquiry (Q): Return current balance in CURBAL field
- Void Authorization (V): Cancel a previous authorization. Must be for same amount as original actual auth; i.e., the amount that was actually authed, not the amount that was requested to be authed.
- Void Sale (VS): Cancel a previous sale transactions (before settlement). Must be for same amount as original sale; i.e., the amount that was available (authorized) in the sale transactions, not the amount that was requested.
- Void Refund (VR): Cancel a previous refund. Amount requested must be for the same amount as original refund request

Table 17.1: Chase Paymentech PNS - Disney Rewards Card Actions

Auth Only Sale (A/S)	*Deposit (D)*	*Refund (R)*	*Balance Inquiry (Q)*	*Void (V) /Void Sale (VS)/ Void Refund (VR)*
Account	Account	Account	Account	Account
Account	Account	Account	Account	Account
Division ID	Division ID	Division ID	Division ID	Division ID
Merchant Order Number	Merchant Order Number	Merchant Order Number		Merchant Order Number
TenderType (R)	TenderType (R)	TenderType (R)	TenderType (R)	TenderType (R)
Class	Class	Class	Class	Class
Exp Date	Exp Date	Exp Date	Exp Date	Exp Date
CVV2	CVV2	CVV2	CVV2	CVV2
First Name	First Name	First Name	First Name	First Name
Last Name	Last Name	Last Name	Last Name	Last Name
Address 1	Address 1	Address 1	Address 1	Address 1
Zip Code	Zip Code	Zip Code	Zip Code	Zip Code
	Authorization Code			

Continued on next page

Table 17.1 – *Continued from previous page*

Auth Only Sale (A/S)	*Deposit (D)*	*Refund (R)*	*Balance Inquiry (Q)*	*Void (V) /Void Sale (VS)/ Void Refund (VR)*
	Authorization Date			

First Name and Last Name are optional and not sent to the processor.

17.2.3 Generally Useful Fields

The following fields are generally useful for most types of transactions. Refer to the on-line field reference list for additional information.

- COMMENT (1 through 4): Four 128-character general-purpose fields. Not sent to Paymentech. Use these for your own tracking purposes.
- CUSTOMER IP ADDRESS: Useful for tracking and fraud purposes when processing e-commerce transactions.
- LAST ACTION SUCCEEDED: Returns "Y" whenever a requested transaction was successful. Otherwise, it returns "N." A useful first check to see if a transaction request was approved.
- RESPONSE CODE: Paymentech's two-digit response code. Note, these are different response codes than returned by the Paymentech Direct/Salem platform.

Additionally, obtain and transmit the card security code (CVV2/CID) information with Conditional Deposit/Sale transactions.

17.2.4 Required PNS Configuration Settings

When connecting to PNS with Trevance® , be sure to tell your Chase Paymentech representative that your account configuration requires:

- Host mode processing.
- Support for ten simultaneous transactions over single socket.
- Auto batch close on PNS side.

These PNS settings are required for Trevance® to operate properly.

17.2.5 Timeouts and Duplicate Detection

If a timeout occurs, Trevance® returns an ASIRESP code of 500 and a non-blank value in the RETRYKEY field. If you decide to resubmit this transaction, you need to send the RETRYKEY field back to Trevance® .

18 First Data Compass Platform

This chapter contains information on configuring processor settings specifically for the First Data Compass platform. First Data is making the Compass system available in several Releases. Trevance® is currently certified for Release 1 functionality. Release 2 functionality includes International Currencies, PayPal, BillMeLater, and Retail. Please contact your First Data representative with any questions regarding schedules for Release 2. This chapter documents the functionality currently available in Compass R1, as well as that scheduled for Compass R2.

Trevance® CN-3500 (batch only) communicates with First Data Compass via S-FTP through the Internet or through a direct connection (VPN or Frame Relay).

Trevance® CN-4200 and CN-4250 communicate with First Data Compass via a dedicated connection (VPN or Frame Relay). Dedicated connections provide highly reliable communication and rapid transaction turn-around times.

Trevance® provides a built-in failover functionality. First Data can provide merchants with additional network-level redundant failover configurations. Please contact your First Data representative for details. Trevance® supports both the First Data On-Line (real-time)

Authorization service and S-FTP batch processing service. Please refer to the Trevance® README file to determine the latest First Data specification to which Trevance® has been certified.

For additional documentation, see the Auric Systems International web site, specifically:

- *General Trevance® Support*
  `http://www.AuricSystems.com/support-center/trevance`

Additional .html reference documents are available your local Trevance® installation's Doc directory.

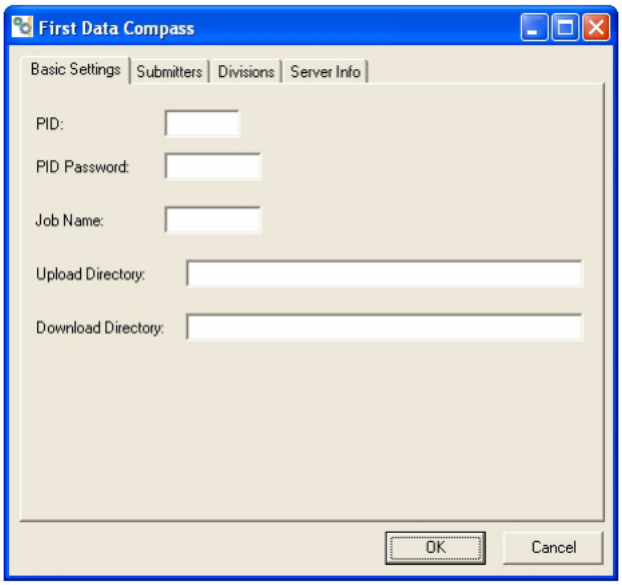
You may also find First Data's 120-byte *Batch Technical Specification* and *On-Line Processing Technical Specification* to be useful. Please contact your First Data representative for copies.

18.1 Configuring Processor Settings

To configure the processor settings:

1. Click on CONFIGURE.
2. If the server isn't paused, click on *PAUSE SERVER TO CONFIGURE ITEMS BELOW*.
3. Click on PROCESSOR SETTINGS to view a screen like the following:

18.1.1 Basic Settings



4. Click on the BASIC SETTINGS tab.

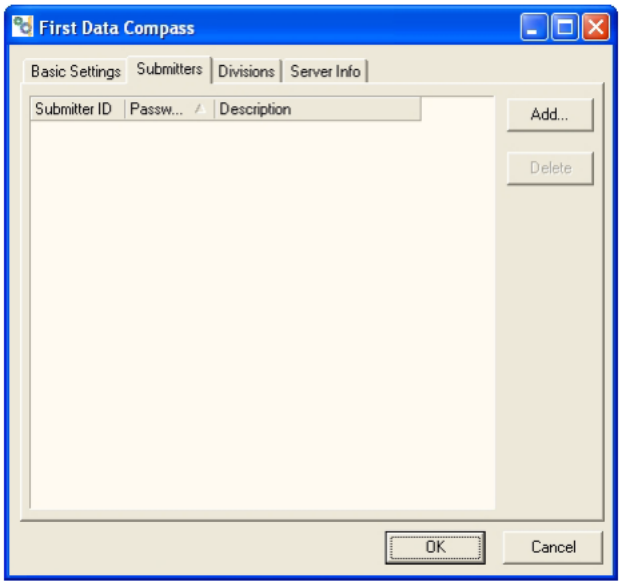
   BASIC SETTINGS information identifies the company presenting the transactions to First Data. In other words, it identifies the company that is running Trevance® .

   This is required information, which comes from First Data.
5. The PID (Presenter ID) identifies your installation.
6. The PID PASSWORD is associated with the Presenter ID.

7. The Job Name identifies your files to the Message Way communications system.
8. The Upload and Download directories need to be entered precisely as they are provided to you by First Data. Note: the path is case sensitive; /send-to-fdc is different from /Send-To-FDC.

18.1.2 Submitters

9. Click on the SUBMITTERS tab to view a screen like the following:



The SUBMITTER ID and PASSWORD identify the company whose transactions are being submitted. Usually, the presenter and submitter companies are the same; however, they may be different for third-party submitters, such as call centers.

At least one submitter is required.

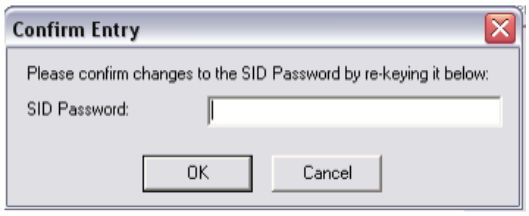
Most installations now use a single submitter ID, even if they are an in-bound call center processing for dozens of clients. Support for multiple submitters is mostly for historic purposes.

The submitters grid is sortable. Click on a heading (SUBMITTER ID, PASSWORD, DESCRIPTION) to change the sort order.

10. To add a submitter, click on

11. Type a number into the Submitter ID box. This number is supplied by First Data and must be entered exactly as supplied. It identifies the company submitting the transactions.

12. Type a password into the PASSWORD box to view:



This is the password associated with the submitter ID (SID)

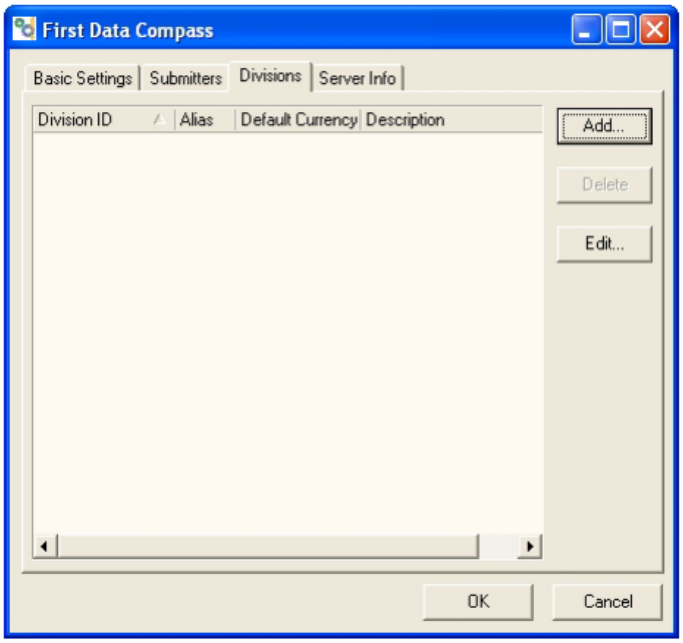
13. Re-enter the password

14. Click on

15. Enter a DESCRIPTION. This description is for your own use in identifying the submitter. The description is never sent to First Data.

18.1.3 Divisions

16. Click on the DIVISIONS tab to view a screen like the following:



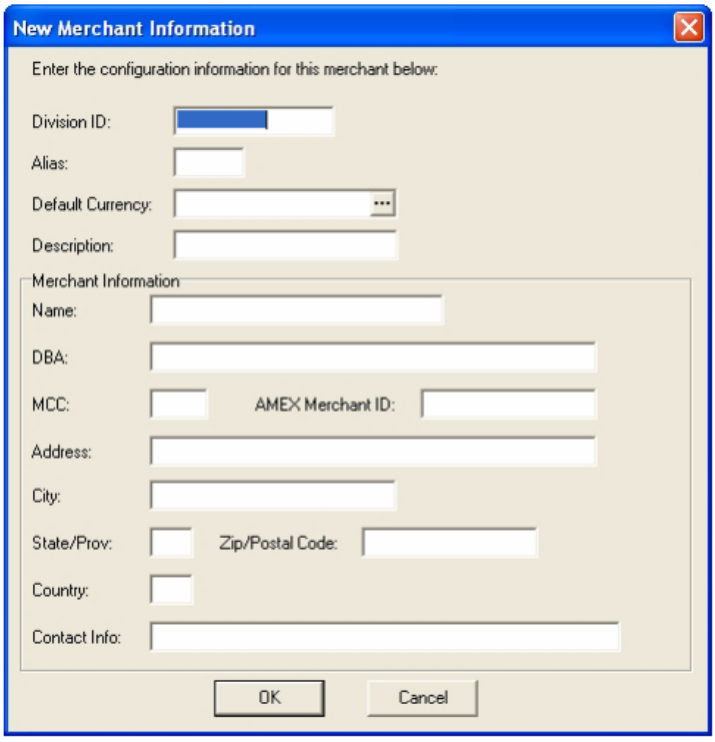
Divisions identify transactions as belonging to different categories, such as the different parts of a large company, mail order/phone order/web sales, or totally different companies (as in the case of an in-bound call center processing for many merchants).

Divisions are also used to process and report on transactions in different currencies. Although First Data allows you to set the currency value with each and every transaction, it is typical, and considered a best practice, to have First Data configure a division for each currency in which you process.

You'll see this information again on when you configure import files. At that time, the division number(s) and associated description(s) are automatically listed under the DEFAULT VALUES tab (in the DIVISION ID box)

The divisions grid is sortable. Click on a heading (DIVISION ID, ALIAS, DEFAULT CURRENCY, DESCRIPTION) to change the sort order.

17. To add a division, click on



18. Type the division number under DIVISION ID. This 10-digit number is supplied by First Data. The number must have 10 digits; if you have a 6-digit number, add four zeroes to the left-hand side (for example, change 123456 to 0000123456).

19. The ALIAS field is provided for future functionality. Leave it blank for now.

20. Under Default Currency, click on ··· to view a list of currencies.

21. Click on the currency you want. Trevance® automatically uses that currency for all transactions associated with that particular division ID.

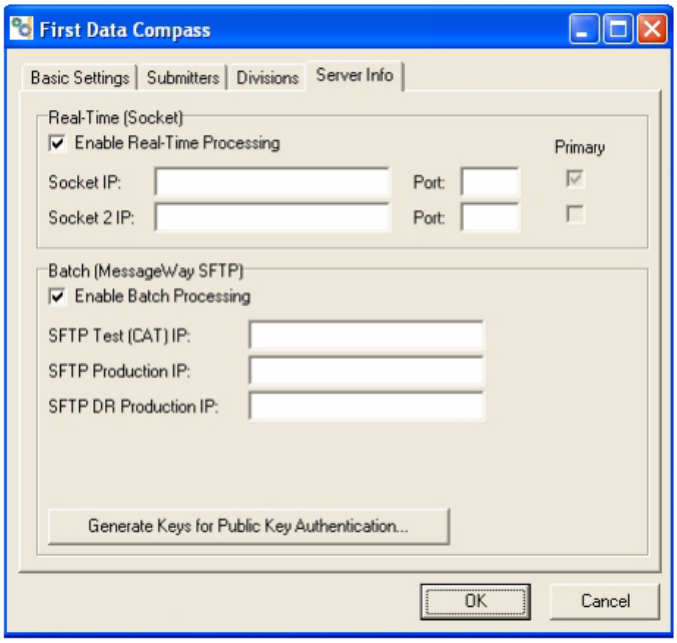
    If you leave the field blank, U.S. dollars are used by default

22. Enter a DESCRIPTION. This description is for your own use in identifying the submitter. The description is never sent to First Data.

23. The Merchant Information section contains your basic merchant info

18.1.4 Server

24. Click on the SERVER INFO tab to view:



The server information is used to configure communications with First Data.

The real-time and batch systems each have their own configuration.

Although most installations perform both real-time and batch operations, you can disable either one if you like. For example, if you already have a batch operation process in place, you can use Trevance® to add real-time operations while continuing to perform your existing batch actions.

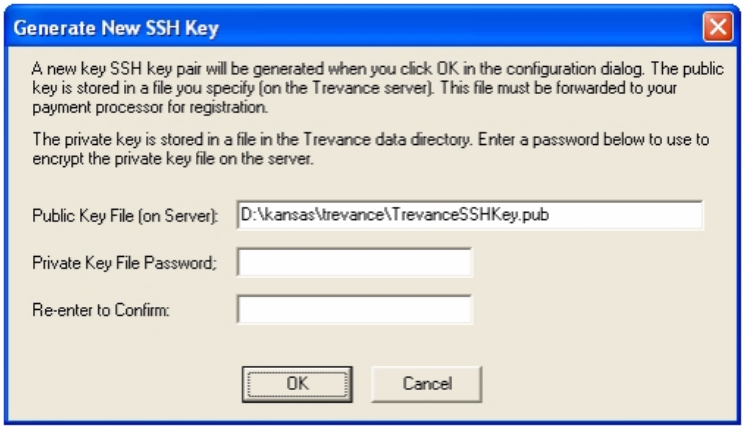
25. Fill in the REAL-TIME (SOCKET) boxes based on information you receive from First Data.

    The IP fields are in the form of "dotted notation" (for example, 192.1.1.42). The real-time interface has a separate socket.

Suppose First Data provides an address that looks like this: 192.1.1.42:8443.

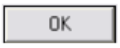
- In the SOCKET IP, type 192.1.1.42.
- In the SOCKET PORT, type 8443.
- Trevance® allows you to optionally configure a primary and failover Socket IP. If you are not configuring failover capabilities, enter only the first Socket IP value.
- Select Primary Socket Connection. This defaults to the first Socket IP address. If you want to select the second as your primary, click the checkbox next to the Socket 2 IP field.
- Fill in the S-FTP boxes based on information you receive from First Data.S-FTP also has both a production, and a fall-back (which First Data calls DR or Disaster Recovery) address.

  First Data may provide an explicit upload and download directory, or they may indicate that you should download or upload from/to the default directory. In this case, enter a period (.) in the Trevance® configuration for that directory.
- Generate your S-FTP public/private keys


Generate New SSH Key
A new key SSH key pair will be generated when you click OK in the configuration dialog. The public key is stored in a file you specify (on the Trevance server). This file must be forwarded to your payment processor for registration.
The private key is stored in a file in the Trevance data directory. Enter a password below to use to encrypt the private key file on the server.
Public Key File (on Server):
D:\kansas\trevance\TrevanceSSHKey.pub
Private Key File Password:
Re-enter to Confirm:
OK
Cancel

- Enter a password for encrypting the private keyfile. This password is stored in the Trevance® database. The private key is generated and stored in the data directory with the name trev-ssh.key. You should make backups of this file.

- Once generated, you'll need to send the Public key to your First Data representative.

- Click on  to complete.

18.1.5 How Failover Works

The Trevance® failover mechanism works as follows:

- When two Socket IP connections are defined, Trevance® uses one as the Primary and one as the Secondary.
- The Primary Connection is indicated by a checkmark in the Server Configuration screen (see above).
- All real-time transactions are sent to the Primary Connection.
- If the Primary Connection is unavailable (disconnected), Trevance® switches to sending transactions to the Secondary Connection.
- If a real-time transaction is sent and never received because the socket disconnects, Trevance® eventually times-out the transaction and returns with a timeout error. Trevance® **does not** automatically retransmit the transaction. The decision to retransmit a real-time transaction is left as a business decision on the merchant side. Retransmitting some transactions (such as debit card authorizations) have monetary consequences.
- If a transaction timeout is received, Trevance® switches connections.
- Primary socket connection can also be set manually without pausing Trevance®Ṡelect Server/Primary Real-Time Socket from the menu and select which socket you want to use as the Primary socket.
- A log entry appears whenever connections are switched.

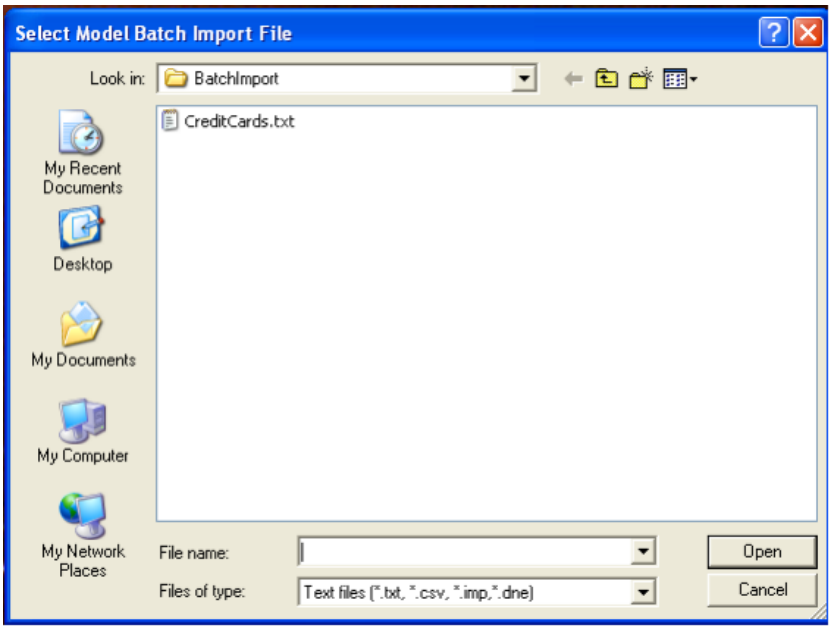
18.2 Configuring Transaction Defaults

This section covers First Data-specific details of batch file and realtime web configuration.

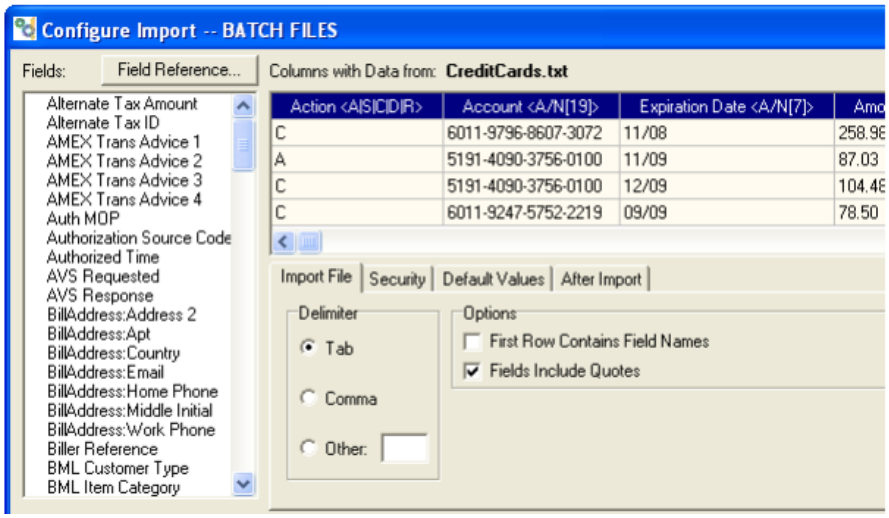
18.2.1 Configure Import Defaults for Batch Files

Refer to"Configuring Imports for Batch File" on page 61 for general information about import configuration.

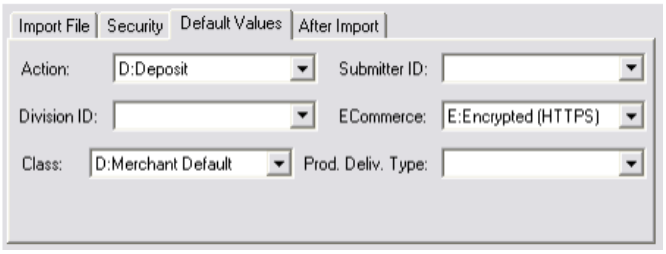
1. Click on CONFIGURE.
2. If the server isn't paused, click on *PAUSE SERVER TO CONFIGURE ITEMS BELOW*.
3. Click on BATCH FILES.
4. Click on BATCHIMPORTS to view:



5. Select the sample CREDITCARDS.TXT file (or any file of your own that you're using for import configuration) to view:



6. Click on DEFAULT VALUES to view:



This screen lets you select default information for Trevance® to use with the transaction if certain fields are missing.

- ACTION for real-time file transactions: AUTHORIZATION is the only action accepted by First Data (and Trevance®) through their system.

  If you are handling a PIN-based debit, you can send a real-time REFUND AUTHORIZATION (RA) transaction. This is considered to be a type of "authorization": a refund authorization.

- ACTION for batch transactions: The two most common default actions are AUTHORIZATION and SALE (also known as conditional deposit).

- DIVISION ID: This is the First Data Division ID that is assumed for all transactions submitted with a division.

- SUBMITTER ID: Batch only. Most current installations have a single submitter ID for all transactions. Select that submitter ID.

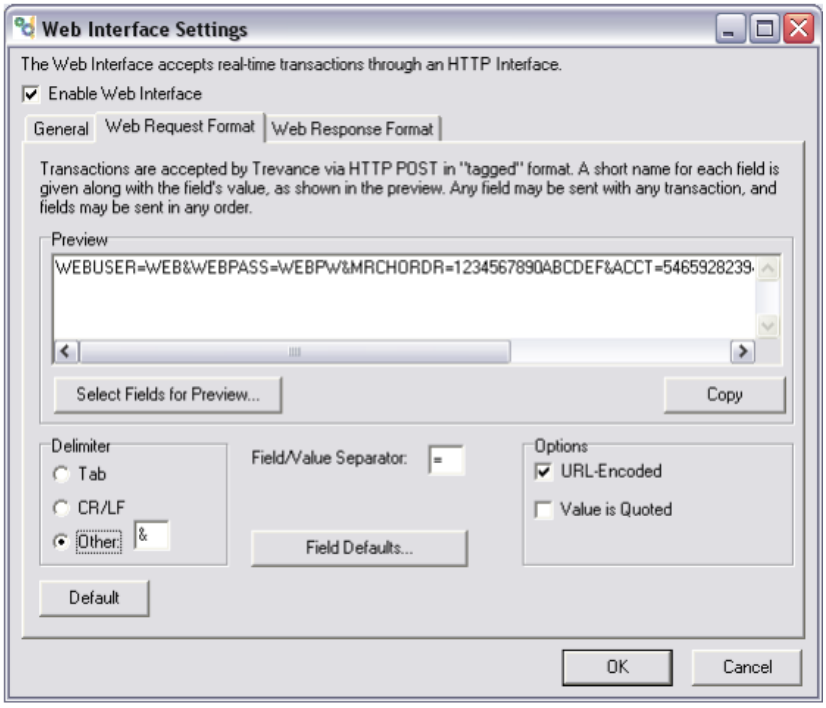
- CLASS: Many merchants have First Data assign a specific transaction class to each division. Select MERCHANT DEFAULT to use the First Data configuration.

- PRODUCT DELIVERY TYPE: Optional field. Leave it blank if you're not sure how to fill it in.

- ECOMMERCE: This field describes the method by which ecommerce transactions are received. The most common is ENCRYPTED (HTTPS), indicating a secured web transaction. You can set a different default value at First Data for each division. If you use that method, select MERCHANT DEFAULT.

18.2.2 Configure Web Transaction Defaults

Refer to"Configuring the Real-Time Web Interface" on page 80 for general information on web transaction configuration.



1. Click on CONFIGURE.
2. If the server isn't paused, click on *PAUSE SERVER TO CONFIGURE ITEMS BELOW*.
3. Click on REAL TIME WEB INTERFACE, then the WEB REQUEST FORMAT tab to view:
4. Click on to view

This screen lets you select default information for Trevance® to use with the transaction if certain fields are missing.

- ACTION: AUTHORIZATION is the only action accepted by First Data (and Trevance®) through their real-time or on-line system.

  If you are handling a PIN-based debit, you can send a real-time REFUND AUTHORIZATION (RA) transaction.This is considered to be a type of "authorization": a refund authorization.

- DIVISION ID: This is the First Data Division ID that is assumed for all transactions submitted with a division.

- SUBMITTER ID: Most current installations have a single submitter ID for all transactions. Select that submitter ID.

- CLASS: Many merchants have First Data assign a specific transaction class to each division. Select MERCHANT DEFAULT to use the First Data configuration.

- PRODUCT DELIVERY TYPE: Optional field. Leave it blank if you're not sure how to fill it in.

- ECOMMERCE: This field describes the method by which ecommerce transactions are received. The most common is ENCRYPTED (HTTPS), indicating a secure web transaction. You can set a different default value at First Data for each division. If you use that method, select MERCHANT DEFAULT.

18.3 Methods of Payment, Actions, and Required Fields

Trevance® for First Data supports the following methods of payment (MOPs):

- Credit card: American Express, Carte Blanche, Delta, Diners Club, Discover, JCB, MasterCard, Novus, Optima, Visa
- Purchase card (level II): American Express, MasterCard, Visa.
- Purchase card (level III): MasterCard, Visa
- Electronic checks: via the Web. (R2)
- PIN-less debit card (R2)

- PIN-based debit card (R2)
- Bill Me Later® (R2)
- PayPal®(R2)
- European debit (R2)

Trevance® automatically recognizes some of these methods of payment.

18.3.1 Important Information about Debit Cards

Debit cards are *not* credit cards. Debit cards must be treated in a significantly different way from credit cards.

The following table lists the most important information about debit cards

Table 18.1: First Data Compass - Debit Card Info

Item	*Applies to PIN-Less*	*Applies to PIN-Based*
"Authorizing" a debit card automatically removes money from the customer's checking account into First Data.	yes	yes
You cannot reverse this"authorization"	yes	no
A "refund authorization" automatically adds money to the customer's checking account.	no	yes
"Depositing" a debit card moves money from First Data's account into your account.	yes	yes
You cannot "void" a debit authorization.	yes	no

Continued on next page

Table 18.1 – *Continued from previous page*

Item	*Applies to PIN-Less*	*Applies to PIN-Based*
You cannot "Auth for a dollar" to verify the debit card is valid. If you try to "Auth for a dollar," you remove $1.00 from the customer's checking account.	yes	yes
You must deposit the exact same amount as you authorized.	yes	yes
If you authorize a debit transaction, the money is removed from the customer's account; but then you have to deposit the "authorized" transaction to put the money in your account. If you don't deposit, the money won't be put into your account.	yes	yes
There is no SALE transaction type–only real-time authorization followed by a batch deposit	yes	no
There is no REFUND transaction.	yes	yes
Authorization codes sometimes return as blank. This is valid behavior.	yes	yes
You can check the LASTACTIONSUCCEEDED or RESPONSE CODE field to determine if the authorization succeeded.	yes	no

18.3.2 Required Information

Regardless of the method of payment, First Data transactions require the following information:

- ACCOUNT: Credit card, debit card, or bank account number.

- ACTION: Authorization, sale, deposit, refund. Set to default or import with each transaction.
- AMOUNT
- DIVISION ID: Set to default or import with each transaction.
- MERCHANT ORDER NUMBER: Every transaction requires a merchant order number. This value is used for tracking transactions through First Data and the Card Associations.

  Merchants should provide a MERCHANT ORDER NUMBER with each transaction. Trevance® generates an order number if one is not provided. If you're performing two-pass authorization transactions that are followed by deposits, you must use the same order number for the deposit *and* for the authorization.
- PRESENTER ID and PASSWORD: Batch only. Configured in Trevance® and never imported.
- SUBMITTER and PASSWORD: Batch only. Usually set to a default value in Trevance® since it is rare to find someone using multiple submitter IDs. If you do use multiple submitter IDs, you must import the submitter ID with each batch transaction. All batch transactions must use the same submitter ID.
- TENDER TYPE: Credit card, purchase card, check, etc. For some transactions–those using credit cards, checks, or Bill Me Later–there's no need to import the tender type. It is a good practice to always import the tender type so you are prepared for new future payment methods that may require the field. The following tables indicate when it's necessary to import the tender type.

The following tables show the minimum additional information that you must send for each method of payment the information that results in your best interchange rate (processing fee). These tables assume you're sending the ACCOUNT, ACTION, AMOUNT, DIVISION ID, and (if necessary) SUBMITTER ID.

Performing basic credit card and check processing with Trevance® for First Data Compass is simple and can be set up quickly. Ask

your First Data representative what is necessary for more complicated transactions.

18.3.3 Generally Useful Fields

The following fields are generally useful for most types of transactions. Refer to the on-line field reference list for additional information.

- COMMENT (1 through 4): Four 128-character general-purpose fields. Not sent to First Data. Use these for your own tracking purposes.
- CURRENCY: Usually set as a default at the division level and not imported.
- CUSTOMER IP ADDRESS: Useful for tracking and fraud purposes when processing e-commerce transactions.
- LAST ACTION SUCCEEDED: Returns "Y" whenever a requested transaction was successful. Otherwise, it returns "N." A useful first check to see if a transaction request was approved.
- RESPONSE CODE: First Data's three-digit response code.
- SOFT DESCRIPTOR (1 and 2): Provides information on the cardholder's monthly statement. This must be set up at First Data before you can use it.

In addition to the fields described above, you should also send the account holder's full name (FIRST NAME and LAST NAME fields) as well as the address, city, state, and ZIP or postal code whenever available. This helps reduce your interchange rate (processing fee). If you do not have a full address, at least obtain and send a ZIP code (U.S.) or postal code (Canada and United Kingdom).

Additionally, obtain and transmit the card security code (CVV2/CID) information with authorization transactions.

18.3.4 Advanced Configuration

The following tables show the basic transaction information for each type of transaction. Once you get beyond the basics, you must consult with your First Data representative to determine what data you should be sending for maximum efficiency and lowest processing fees (also called interchange).

First Data's *On-Line Processing Technical Specification and Batch Technical Specification* describe over 160 possible fields that can be transmitted. The specific fields you should send will depend on your market type, your business class (e-commerce, MOTO, recurring, IVR, retail, and so on), and the forms of payment you accept (credit card, purchase card, check, debit, Bill Me Later, and so on). Working with your First Data representative is the quickest way to determine which fields you should send.

Table 18.2: First Data Compass Credit Card

Authorization	*Auth Reversal*	*Deposit*	*Sale*	*Refund*
Exp Date	Exp Date	Exp Date	Exp Date	Exp Date
	Auth Date	Auth Date		
	Auth Date	Auth Date		

Account Check	*Partial Auth*	*Force Full Auth*
Exp Date	Exp Date	Exp Date

Continued on next page

Table 18.3 – *Continued from previous page*

Account Check	*Partial Auth*	*Force Full Auth*

Transactions that contain the minimum information plus an expiration date are automatically identified as "credit card" transactions. Sending a "C" in the TENDER TYPE field explicitly identifies credit card transactions.

Credit card account values can contain spaces or dashes ("-"). First Data recommends returning the original RESPONSE CODE (which will typically be 100) with all deposit transactions.

Authorization Reversals require the Authorized Amount to be included in the reversal. Action Code for Auth Reversals is L.In the Amount (AMT) field send the amount that was originally authorized.

Authorization Reversals are supported for Visa, MasterCard, and MC Diners.

Partical Authorization is supported for American Express, MasterCard, and Visa. You account must be set up to support this transaction. Action code for Partial Authorization is PA.

In a Partial Authorization, the credit card is authorized for the maximum available credit up to and including the requested amount. If you attempt to authorize $100.00 and the card has only $75 available, the Partial Authorization will succeed, but only for the $75.00.

If you use Partial Authorization, or if you have a division configured to default to Partial Authorization, you must track the Total Authorized Amount (AUTHAMT) response field from Trevance®.This field returns the actual amount that was authorized.

There is a new ASIRESP code of 105 indicating a Partial Authorization occurred.

When performing a deposit, refund, or auth reversal, you need to use the value returned in AUTHAMT.

Note that, if you have a division configured to default to Partial Authorization, the Sales transactions sent through the real-time interface will default to Partial Auth, but sales transactions sent through the batch interface will default to Full Auth.

The reason is that First Data does not support Partial Auth for Sales (Conditional Deposit) transactions. And First Data only supports Auths through the real-time interface. However, when using the Trevance® CN-4250, Trevance® first Authorizes the transaction through the realtime interface (which supports Partial Auth) and, if successful, batches a Deposit transaction for end of day settlement.

Trevance® also supports the Full Authorization (FA) action which forces a transaction to fail if the amount requested for authorization is not available. FA must only be used where a division is set up to support Partial Authorizations; otherwise use the standard Authorized (A) action code.

The new (June 2009) Account Check (Y) action code is supported for MasterCard and Visa transactions. Sending an Account Check (Y) with a zero (0) dollar amount verifies the existence of the card. Previously, merchants would typically send a dollar auth that was never deposited. Visa now requires all such transactions to now be Account Checks. MasterCard supports this only for Recurring Billing transactions.

When Trevance® receives an Auth transaction with a zero dollar amount, and the method of payment is either MasterCard or Visa, it converts that into an Account Check (Y) action. Zero amounts for all other methods of payment are passed directly to First Data.

Table 18.4: First Data Compass - Purchase Card (Level ll)

Authorization	*Auth Reversal*	*Deposit*	*Sale*	*Refund*
Exp Date	Exp Date	Expiration Date	Expiration Date	Exp Date

Continued on next page

Table 18.4 – *Continued from previous page*

Authorization	*Auth Reversal*	*Deposit*	*Sale*	*Refund*
	Auth Date	Purchase Order Number	Purchase Order Number	
		Ship To Address (AM)	Ship To Address (AM)	
		Tender Type	Tender Type	
		Authorization Code		
		Authorization Date		

Purchase card (level II) transactions require the same minimum information as a credit card transactions, plus several additional fields.

American Express, MasterCard, and Visa accept level II transactions.

Purchase Card account values can contain spaces or dashes ("-").

You must explicitly identify Purchase Card transactions by importing "P" in the TENDER TYPE field.

You must provide the amount of tax, even if it is $0.00.

You should provide the SHIP TO ADDRESS fields (ADDRESS, CITY, STATE, ZIP) for American Express (AM) purchase card transactions.

Table 18.5: First Data Compass - Purchase Card (Level lll)

Auth	*Auth Reversals*	*Deposit*	*Sale*	*Refund*

Continued on next page

Table 18.5 – *Continued from previous page*

Auth	*Auth Reversals*	*Deposit*	*Sale*	*Refund*
Exp Date	Exp Date	Expiration Date	Expiration Date	Exp Date
	Auth Date	Purchase Order Number	Purchase Order Number	
	Auth Code	Tax	Tax	
		Alternate Tax Amount (MC)	Alternate Tax Amount (MC)	
		Alternate Tax ID (MC)	Alternate Tax ID (MC)	
		Discount	Discount	
		Tender Type	Tender Type	
		Authorization Code		
		Authorization Code		

Purchase card (level III) transactions require the same minimum information as level II transactions, plus several additional fields. Some fields are required only for a specific card type (MC) and are so marked in the chart.

Trevance® supports supplemental records for purchase card (level III) line items. Please see "Appendix B. Level III Transactions" on page 353.

MasterCard and Visa accept level III transactions. You must explicitly identify Purchase Card transactions by importing "P" in the TENDER TYPE field.

American Express provides a similar functionality through the use of four American Express TRANSACTION ADVICE ADDENDUM

fields. The field reference list gives details on how these fields are used.

Table 18.6: First Data Compass - Electronic Checks

Authorization	*Deposit*	*Sale*	*Refund*
Routing Number	Routing Number	Routing Number	Routing Number
BillAddress: First Name	BillAddress: First Name	BillAddress: First Name	BillAddress: First Name
BillAddress: Last Name	BillAddress: Last Name	BillAddress: Last Name	BillAddress: Last Name

Transactions that contain the minimum information plus a ROUTING NUMBER (also called a bank ID or bank routing number) are automatically identified as electronic checks (eChecks). Trevance® allows you to accept checks electronically (that is, over a secure web interface).

This type of transaction is not designed for handling accounts receivable conversion (ARC) or point of purchase (POP) check conversions.

Place the checking account number in the ACCOUNT field and the Routing Number (Bank ID or Bank Routing Number) in the ROUTING NUMBER field.

The ACCOUNT field can contain spaces. It must *not* have dashes "-").

Table 18.7: First Data Compass - PIN-less Debit

Authorization	*Auth Reversal*	*Deposit*	*Sale*	*Refund*
Expiration Date	Expiration Date	Expiration Date		

Continued on next page

Table 18.7 – *Continued from previous page*

Authorization	*Auth Reversal*	*Deposit*	*Sale*	*Refund*
Biller Reference	Biller Reference		N/A	N/A
Tender Type	Tender Type	Tender Type		
		Authorization Code		
		Authorization Code		

PIN-less debit is also known as debit bill payment and is only available to select industries, including utilities, insurance, telecommunications, cable, financial, and government entities. Regulations currently do not allow PIN-less debit to be used for recurring or installment payments.

The PIN-less debit is a single-message transaction. As soon as the transaction is "authorized," money is removed from the customer's account. First Data takes the debit authorization data and stores it in a Debit Database. When you send a deposit transaction in the daily batch file, First Data matches the deposit against the Debit Database. When a match occurs, money moves to your account. If no match occurs, First Data reports the exception to the merchant.

Debit authorization (A) and Sale (S) transactions must occur through the real-time interface.

An exception to the above is that recurring Auth and Sale transactions may be submitted via batch. This requires the Recurring flag to be passed with the transaction. This functionality allows PINless debit cards to be used for recurring payment purposes. The very first transaction still must go through the real-time interface. k

Online Deposit and Sale transactions require a Trevance® CN-4250.

Trevance® cannot automatically recognize a PIN-less debit transaction because the fields passed for PIN-less debit are iden-

tical to the fields passed for a credit card transaction, and some cards can be used for both credit and debit.

You must include the"L" TENDER TYPE in all PIN-less debit transactions. If you do not provide the TENDER TYPE field, the transaction is processed as a credit card.

Authorization Reversals must be submitted within 90 minutes of the Authorization transaction.

Table 18.8: First Data Compass - Bill Me Later

Authorization	*Deposit*	*Sale*	*Refund*
BML Customer Type	BML Customer Type	BML Customer Type	BML Customer Type
BML Item Category	BML Item Category	BML Item Category	BML Item Category
Product Type		Product Type	
Date of Birth[2]		Date of Birth[2]	
T and C Version[1]	T and C Version	T and C Version [1]	T and C Version
Freight	Freight	Freight	Freight
Customer Registration Date	Customer Registration Date	Customer Registration Date	Customer Registration Date
Customer Social Security Number[2,3]	Authorization Code	Customer Social Security Number[2,3]	
Bill Address: First Name	Authorization Date	Bill Address: First Name	
Bill Address: Last Name		Bill Address: Last Name	

Continued on next page

Table 18.8 – *Continued from previous page*

Authorization	*Deposit*	*Sale*	*Refund*
Bill Address: Last Name		Bill Address: Last Name	
Bill Address: City		Bill Address: City	
Bill Address: State/Province		Bill Address: State/Province	
Bill Address: Zip/Postal Code		Bill Address: Zip/Postal Code	
Bill Address: Country[4]			
Ship Address: Last Name		Ship Address: Last Name	
Ship Address: City		Ship Address: City	
Ship Address: State/Province		Ship Address: State/Province	
Ship Address: Zip/Postal Code		Ship Address: Zip/Postal Code	

BML classifies authorization requests as being of three types:

- Var D: Using dummy account numbers
- Var A1: Real account number stored from previous purchase for existing customer (WEB)
- Var A2: Real account number plus further identifying information (Call Centers)

NOTES:
[1]Var D only
[2]Var D and Var A2 only
[3]Last four digits of social security number only
[4]Must be "US"

Trevance® automatically identifies "Bill Me Later" transactions.

Refer to the on-line field reference list for details on the specific fields.

Table 18.9: First Data Compass - European Direct Debit

Authorization	*Deposit*	*Sale*	*Refund*
EDD Country Code	EDD Country Code	EDD Country Code	EDD Country Code
EDD Bank Sort Code	EDD Bank Sort Code	EDD Bank Sort Code	EDD Bank Sort Code
EDD RIB Code (optional)	EDD RIB Code (optional)	EDD RIB Code (optional)	EDD RIB Code (optional)
	Bill Address: First Name	Bill Address: First Name	Bill Address: First Name
	Bill Address: Last Name	Bill Address: Last Name	Bill Address: Last Name

The EDD Country Code (EDCNTRY) indicates the country in which the customer's bank is located. It must be one of the following:

- AT Austria
- BE Belgium
- FR France

- DE Germany
- NL Netherlands
- GB United Kingdom

The EDD Bank Sort Code (EDBSC) identifies the customer's bank. Each country has its own bank sort code format.

The EDD RIB Code (EDRIB) is the bank account checksum. This is optional and used only in France.

18.3.5 PayPal

Trevance® supports PayPal transactions through both the real-time and batch interfaces. Note that the Trevance® CN-4250 provides support for real-time transaction types not supported by First Data (such as Sale, Capture, and Refund) by converting the real-time request into a queued batch transaction.

Auric appreciates your setting the ButtonSource parameter in your initial call to the PayPal website to: AURICCN_EXPRESS_ECUS PayPal transactions require integration with the PayPal website.To support PayPal transactions with Trevance® you first send one of the Set transactions (for example, SA) to Trevance®.Trevance® makes a call to First Data which returns a PayPal token on success. Trevance® returns this value in the PYTOKEN field.

Using this token, you redirect the customer to the PayPal site. When the customer has completed authentication, PayPal sens the customer back to your site (to the RTRNURL parameter you send with the initial Set). At this opint, you can use the token value to complete the transaction through First Data using Trevance® transactions.

All PayPal transactions must provide the following fields:

- AMT (Amount)
- DIVISION
- TENDTYPE (Tender type): Set to: Y
- MRCHORDR (Merchant Order Number)
- ACTION (Action Code)

The following shows:

- Action: an English-language description of the transasction type.
- Trevance® Action: The ACTION sent to Trevance® .
- Required Fields: Fields required to be sent with this transaction, in addition to the standard fields documented above.
- Online and Batch: First Data action (or action taken by Trevance® for transactions that are handled locally).

  First line names the PayPal Express Checkout action. Second line shows the First Data Method of Payment along with First Data's Subtype. For example, a notation of ES/A indicates this is First Data Action Code ES subtype A.

Table 18.10: First Data Compass - Pay Pal

Action	*Trevance® Action*	*Required Fields*	*Online*	*Batch*
Set for Auth	SA	RTRNURL CNCLURL	Set Express Payment ES/A	
Set for Order	SO	RTRNURL CNCLURL	Set Express Payment ES/O	
Set for Billing Agreement	SC	RTRNURL CNCLURL	Set Express Payment ES/C	
Set for Auth w/ Billing Agreement	SB	RTRNURL CNCLURL	Set Express Payment ES/B	
Set for Order w/ Billing Agreement	SE	RTRNURL CNCLURL	Set Express Payment ES/E	

Continued on next page

Table 18.10 – *Continued from previous page*

Action	*Trevance® Action*	*Required Fields*	*Online*	*Batch*
Get for Auth	GA	PYTOKEN	Get Express Payment EG/A	
Get for Order	GO	PYTOKEN CNCLURL	Get Express Payment EG/O	
Get for Billing Agreement	GC	PYTOKEN	Get Express Payment EG/O	
Get for Auth w/ Billing Agreement	GB	PYTOKEN	Get Express Payment EG/B	
Get for Order w/ Billing Agreement	GE	PYTOKEN	Get Express Payment EG/E	
Auth	A	PYTOKEN PYPAYER	Do Express Payment ED/A	
Auth from Order	A	PYORDR	Do Auth AU/O	Do Auth AU/O
Auth from Contract	A	PYCID	Do Reference AU/B	Do Reference AU/B
Reauth	A	PYTID	Do Re-Auth AU/A	Do Re-Auth AUA
Auth w/Billing Agreement	AB	PYTOKEN PYPAYER	Do Express Payment ED/B	

Continued on next page

Table 18.10 – *Continued from previous page*

Action	*Trevance® Action*	*Required Fields*	*Online*	*Batch*
Auth from Order with Billing Agreement	AE	PYORDR	Do Auth AU/E	Do Auth AU/E
Sale	S	PYTOKEN PYPAYER	Do Express Payment ED/A Queue to batch on success as Do Capture RG/P	
Sale	S	PYCID		Recurring Sale RG/R
Refund (Memo)	R	CAPDATE PYTID		Memo Post Refund RD/M
Refund	R	PYTID	Queued to Batch	Full Refund RD/F
Partial Refund	PR	PYTID	Queued to Batch	Partial Refund RD/P
Capture	D	PYTID	Queued to Batch	Do Capture RG/P
Capture (Memo)	D	CAPDATE PYTID		Memo Post Sale RG/M
Final Capture	FD	PYTID	Queued to Batch	Do Capture RG/F

Continued on next page

Table 18.10 – *Continued from previous page*

Action	*Trevance® Action*	*Required Fields*	*Online*	*Batch*
Auth Reversal	L	PYTID	Do Void AR/A	Do Void AR/A
Order Reversal	L	PYORDR	Do Void AR/O	Do Void AR/O
Auth Reversal w/ Billing Agreement	LB	PYTID	Do Void AR/B	Do Void AR/B
Order Reversal w/ Billing Agreement	LE	PYORDR	Do Void AR/E	Do Void AR/E
Create Order	OO	PYTOKEN PYPAYER	Do Express Payment ED/O	
Order From Contract	OO	PYCID	Do Reference AU/E	Do Reference AU/E
Create Billing Agreement	OC	PYTOKEN PYPAYER	Do Express Payment ED/C	
Create Order w/ Billing Agreement	OE	PYTOKEN PYPAYER	Do Express Payment ED/E	
Mass Pay PENDING	MP			Mass Pay RG/S

Continued on next page

Table 18.10 – *Continued from previous page*

Action	*Trevance® Action*	*Required Fields*	*Online*	*Batch*
Void	V	PYTID	Remove Previous Sale, Capture, or Refund Transaction from Queued batch. Must be sent prior to batch settlement	

18.3.5.1 PayPal Process Flow

The PayPal process flow can be thought of in the following phases:

- Initiation
- Authentication
- Authorization
- Capture

Initiation, Authorization, and Capture occur through the Trevance® interface to First Data. Authentication occurs on the web through interaction with the PayPal site.

A typical sale transaction would be as follows:

- SA (Set for Auth): Get back a PYTOKEN
- Redirect to PayPal web site for authentication. Use the PYTOKEN value as the PayPal Token parameter.
- GA (Get for Auth): Get customer information (name, shipping address, etc.) as well as PYPAYER.
- Auth (Authorise): Get back a PYTID.
- D (Capture): Capture the authorization using the PYTID returned by the Auth. Get back a different PYTID which refers to the capture itself.

You can also work with Orders, which allow multiple authentication:

- SO: Set for Order. Get back a PYTOKEN.
- Redirect to PayPal web site for authentication. Use the PYTOKEN value as the PayPal Token parameter.
- GO (Get for Order): Get customer information (name, shipping address, etc.) as well as PYPAYER.
- OO (Create Order): Get back a PYORDR value.
- A (Authorise from Order): Get back a PYTID.
- D (Capture): Capture the authorization using the PYTID returned by the Auth. Get back a different PYTID which refers to the capture itself.

You can create contracts:

- SC: Set for Contract. Get back a PYTOKEN.
- Redirect to PayPal web site for authentication. Use the PYTOKEN value as the PayPal Token parameter.
- GC (Get for Contract): Get customer information (name, shipping address, etc.) as well as PYPAYER.
- OC (Create Billing Agreement): Get back a PYCID value.
- A (Authorise from Contract): Get back a PYTID.
- D (Capture): Capture the authorization using the PYTID returned by the Auth. Get back a different PYTID which refers to the capture itself.

  You could also create an order from contract and then auth/capture against that.

In order to simplify recurring billing, First Data has a Recurring Sale transaction which is available only in Batch mode. Trevance® implements this Recurring Sale as an S transaction.

Note that the S transaction for the real-time/web works differently from the S transaction for batch.

When doing refunds, the PYTID returned from the Capture must be used. Note that this PYTID is only returned from the batch interface, not the web interface as First Data does not support real-time capture.

Get returns customer information in the usual fields you would send to First Data for a credit card or check transaction: BILLFNAM, BILLLNAMe, BILLEMAL, etc.)

Table 18.11: First Data Compass - Retail Credit Card Swipe

Authorization	*Deposit*	*Sale*	*Refund*
Track 1 or Track 2	Account	Track 1 or Track 2	Account
	Expiration Date		Expiration Date
	Authorization Date		
	Authorization Code		

Trevance® automatically recognizes "retail credit card swipe" transactions.

Either TRACK 1 or TRACK 2 data can be provided. If both are provided, Trevance® uses TRACK 1 since it contains more data.

During authorization, Trevance® extracts the account and expiration date from the track data and returns it in the ACCOUNT and EXPIRATION fields. Merchants must remember this data for later submission to Trevance® in a deposit or refund transaction. You must not store track data after the authorization is complete. Trevance® in compliance with Card Association rules, does not export the track data after processing

Table 18.12: First Data Compass - Retail Credit Card: Manually Entered

Authorization	*Deposit*	*Sale*	*Refund*
Expiration Date	Expiration Date	Expiration Date	Expiration Date
Zip Code	Zip Code	Zip Code	Zip Code
Class	Class	Class	Class
	Authorization Date		
	Authorization Code		

Manually entered retail credit card transactions look very much like card-not-present credit card transactions.

You must provide the minimum information plus the card's EXPIRATION DATE and ZIP CODE (postal code).

Manually entered retail credit card transactions must import a "P" in the TRANSACTION CLASS field.

19 Transfirst

This chapter contains information on configuring processor settings *specifically for TransFirst.*. Please refer to "Part I. Trevance® Installation, Configuration, and Operation" in this manual for generic Trevance® information.

Trevance® supports secure HTTPS real-time and SFTP batch connections to the TransFirst CNP platform.

For additional documentation, see the Auric Systems International web site, specifically:

- *General Trevance® Support*
  http://www.AuricSystems.com/support-center/trevance

Additional technical HTML reference documents are available in your local Trevance® Doc directory.

You may also find TransFirst's Managed eLink and Batch Technical specifications to be useful. Please contact your TransFirst representative for copies.

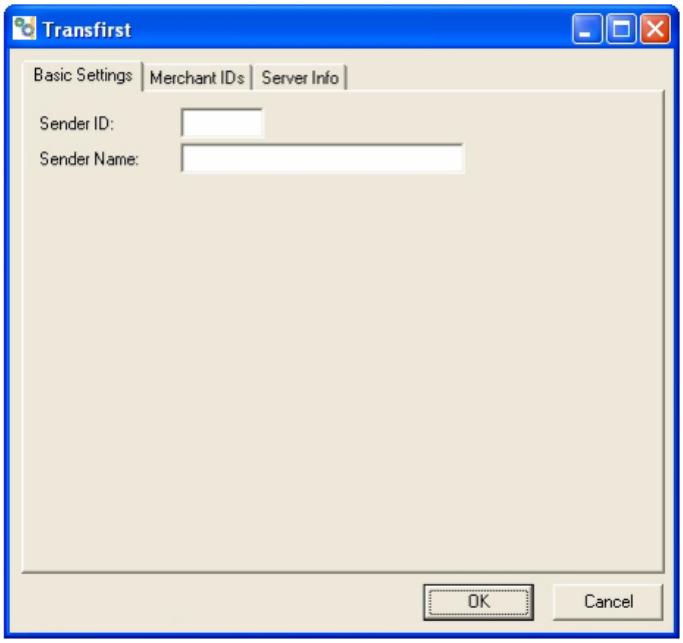
19.1 Configuring Processor Settings

To configure the processor settings:

1. Click on CONFIGURE.

2. If the server isn't paused, click on *PAUSE SERVER TO CONFIGURE ITEMS BELOW*.

3. Click on PROCESSOR SETTINGS to view a screen like the following:



19.1.0.2 Basic Settings

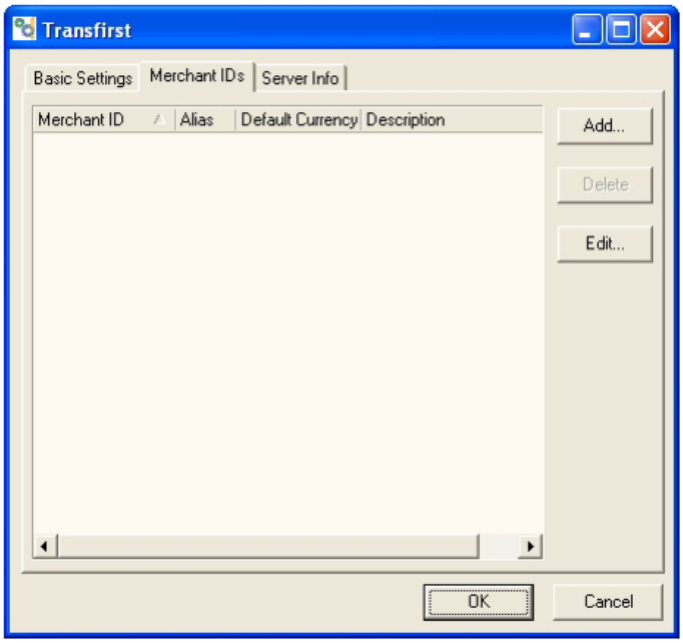
4. Click on the BASIC SETTINGS tab.

   BASIC SETTINGS information identifies the company presenting information to TransFirst. In other words, it identifies the company that's running Trevance®.

   This is required information, which comes from TransFirst.

19.1.0.3 Merchant Numbers

5. Click on the MERCHANT NUMBERS tab to view a screen like the following:

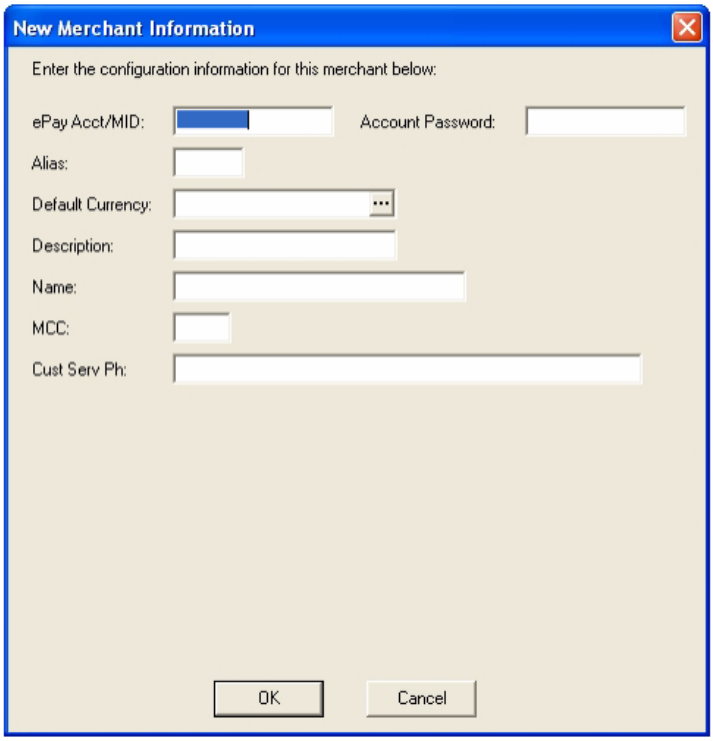


Merchant Numbers (which TransFirst also calls Merchant IDs or ePay Account IDs) identify transactions as belonging to different categories, such as the different parts of a large company, mail order/phone order/web sales, or totally different companies (as in the case of an in-bound call center processing for many merchants).

You'll see the information in this screen again when you configure import files. At that time, the Merchant Number(s) and associated description(s) are automatically listed under the DEFAULT VALUES tab (in the MERCHANT NUMBER box).

6. To add a Merchant, click on

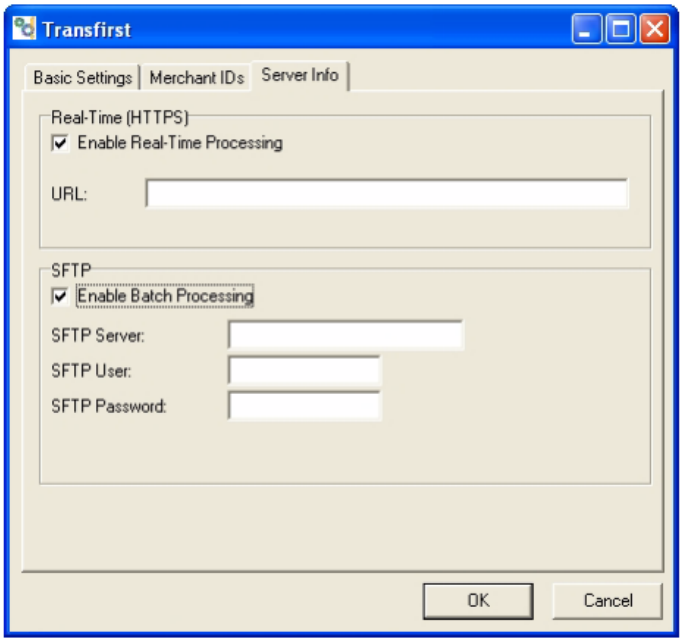
to view:



7. In the EPAYACCT/MID field, type the value provided to you by TransFirst.
8. The ALIAS field is provided for future functionality. Leave it blank for now.
9. Under Default Currency, click on ··· to view a list of currencies. Currently, only US Dollars are supported through TransFirst.
10. Enter a DESCRIPTION. This description is for your own use in identifying the submitter. The description is never sent to TransFirst.
11. Enter the merchant information and MCC value provided by TransFirst.
12. Enter the Customer Service Phone number. This value is sent to TransFirst.
13. Click on OK

19.1.0.4 Server Info

14. Click on the SERVER INFO tab to view:



The server information helps set up communications with TransFirst.

15. Fill in the boxes based on information you receive from TransFirst.
16. Click on

19.2 Methods of Payment, Actions, and Required Fields

Trevance for TransFirst supports the following methods of payment (MOPs):

- Credit card: American Express, Carte Blanche, Diners Club, Discover, JCB, MasterCard, Visa
- Purchase card (level II): American Express, MasterCard, Visa.

- Electronic Checks.

Trevance® automatically recognizes some of these methods of payment. For others, specific fields must be set. Refer to the "Method of Payment" documentation in the *Trevance® Field Reference for TransFirst* (http://www.AuricSystems.com/tr_transfirst).

19.2.1 Required Information

Regardless of the method of payment, TransFirst transactions require the following information:

- ACCOUNT: Credit card, debit card, or bank account number.
- ACTION: Authorization, sale, deposit, refund. Set to default or import with each transaction.
- AMOUNT
- MERCHANT NUMBER: Set to default or import with each transaction
- MERCHANT ORDER NUMBER: Every transaction requires a merchant order number. This value is used for tracking transactions through Trevance® and the Card Associations.

  Merchants should provide a MERCHANT ORDER NUMBER with each transaction. Trevance® generates an order number if one is not provided. If you're performing two-pass authorization transactions that are followed by deposits, you must use the same order number for the deposit *and* for the authorization. A unique order number for each transaction helps reporting and reconciliation, but is not mandatory for TransFirst.
- TENDER TYPE: Credit card, purchase card, check, etc. For some transactions—those using credit cards – there's no need to import the tender type. It is a good practice to always import the tender type so you are prepared for new future payment methods that may require the field. The following tables indicate when it's necessary to import the tender type.

The following tables show the minimum additional information that you must send for each method of payment–not the in-

formation that results in your best interchange rate (processing fee). These tables assume you're sending the ACCOUNT, ACTION, AMOUNT, and MERCHANT NUMBER.

Trevance® supports hundreds of different import/export fields in order to support a wide variety of payment types for a number of different payment processors. As most merchants start out processing just credit cards, there's a fairly small number of fields that must be used. If you find yourself importing over a dozen fields, please call your Auric representative to ensure you're not doing more work than you need to

Performing basic credit card processing with Trevance® for TransFirst is simple and can be set up quickly. Ask your Trevance® representative what is necessary for more complicated transactions

19.2.2 TransFirst-Specific Considerations

The following are a few things to consider when connecting with TransFirst:

- Only Sales (S) and Refund (R) transactions are supported for Electronic Checks.
- For batch files, either the Tax Amount must be sent, or the Tax Exempt Flag sent and set to Y for authorizations.
- TransFirst defines ECommerceType differently than other processors. For TransFirst, ECommerceType is not sent except for 3DS transactions; for 3DS transactions, it must be set to the numeric value obtained at authorization time. This is passed through directly.

Table 19.1: Trans First - Credit Card

Authorization	*Deposit*	*Sale*	*Refund*
Expiration Date	Expiration Date	Expiration Date	Expiration Date

Continued on next page

Table 19.1 – *Continued from previous page*

Authorization	*Deposit*	*Sale*	*Refund*
	Authorization Date		
	Authorization Code		

Transactions that contain the minimum information plus an expiration date are automatically identified as "credit card" transactions.

Sending a "C" in the TENDER TYPE field explicitly identifies credit card transactions.

Credit card account values can contain spaces or dashes ("-")..

Table 19.2: Trans First - Purchase Card (Level ll)

Authorization	*Deposit*	*Sale*	*Refund*
Expiration Date	Expiration Date	Expiration Date	Expiration Date
	Purchase Order Number	Purchase Order Number	
	Tax	Tax	
	Ship To Address (AM)	Ship To Address (AM)	
	Tender Type	Tender Type	
	Authorization Code		

Continued on next page

Table 19.2 – *Continued from previous page*

Authorization	*Deposit*	*Sale*	*Refund*
	Authorization Date		

Purchase card (level II) transactions require the same minimum information as a credit card transactions, plus several additional fields.

American Express, MasterCard, and Visa accept level II transactions.

Purchase Card account values can contain spaces or dashes ("-").

You must explicitly identify Purchase Card transactions by importing "P" in the TENDER TYPE field.

You must provide the amount of tax, even if it is $0.00.

TransFirst recommends providing the SHIP TO ADDRESS fields (ADDRESS, CITY, STATE, ZIP) for American Express (AM) purchase card transactions.

Table 19.3: Trans First - Electronic Checks

Sale	*Refund*
Routing Number	Routing Number
BillAddress: First Name	BillAddress: First Name
Bill Address: Last Name	Bill Address Last Name

Transactions that contain the minimum information plus a ROUTING NUMBER (also called a bank ID or bank routing number) are automatically identified as electronic checks (eChecks).

Trevance® allows you to accept checks electronically (that is, over a secure web interface).

This type of transaction is designed for eCommerce-style checks; it is not designed for handling accounts receivable conversion (ARC) or point of purchase (POP) check conversions..

Place the checking account number in the ACCOUNT field and the Routing Number (Bank ID or Bank Routing Number) in the ROUTING NUMBER field.

The ACCOUNT field can contain spaces. It must not have dashes ("-").

19.2.3 Generally Useful Fields

The following fields are generally useful for most types of transactions. Refer to the on-line field reference list for additional information.

- COMMENT (1 through 4): Four 128-character general-purpose fields. Not sent to payment processor. Use these for your own tracking purposes.
- CURRENCY: Usually set as a default at the merchant number level and not imported. Any imported value overrides the default.
- CURRENCY: Usually set as a default at the merchant number level and not imported. Any imported value overrides the default.
- LAST ACTION SUCCEEDED: Returns "Y" whenever a requested transaction was successful. Otherwise, it returns "N." A useful first check to see if a transaction request was approved.
- RESPONSE CODE: Payment Processor's response code.
- SOFT DESCRIPTOR (1 and 2): Provides information on the cardholder's monthly statement. This must be set up at TransFirst before you can use it.

In addition to the fields described above, you should also send the account holder's full name (FIRST NAME and LAST NAME fields) as well as the address, city, state, and ZIP or postal code

whenever available. This helps reduce your interchange rate (processing fee). If you do not have a full address, at least obtain and send a ZIP code (U.S.) or postal code (Canada and United Kingdom).

Additionally, obtain and transmit the card security code (CVV2/CID) information with authorizations.

Your TransFirst representative can help you choose what set of fields best fits your requirements.

19.3 Advanced Transaction Configuration

The preceding tables showed the basic transaction information for each type of transaction. Once you get beyond the basics, you must consult with your TransFirst representative to determine what data you should be sending for maximum efficiency and lowest processing fees (also called interchange).

The TransFirst specifications describe over 100 possible fields that can be transmitted. The specific fields you should send will depend on your market type, your business class (e-commerce, MOTO, recurring, IVR, etc.), and the forms of payment you accept (credit card, purchase card, etc.). Working with your TransFirst representative is the quickest way to determine which fields you should send.

20 Tsys

If you don't configure processor settings correctly, Trevance® refuses to work in production mode; it remains paused. You may see a warning message on your screen.

Tsys was formerly known as First National Merchant Solutions. This chapter contains information on configuring processor settings *specifically for First National Merchant Solutions (FNMS)* Please refer to "Part I. Trevance® Installation, Configuration, and Operation" in this manual for generic Trevance® information.

Trevance® CN-3500 supports VPN and Frame connections to FNMS. For additional documentation, see the Auric Systems International web site, specifically:

- *General Trevance® Support*
  http://www.AuricSystems.com/support-center/trevance

Additional .html reference documents are available in your local Trevance® Doc directory.

You may also find Paymentech's 120-byte *Batch Technical Specification and On-Line Processing Technical Specification* to be useful. Please contact your Paymentech representative for copies.

20.1 Configuring Processor Settings

To configure the processor settings:

1. Click on CONFIGURE.
2. If the server isn't paused, click on *PAUSE SERVER TO CONFIGURE ITEMS BELOW*.
3. Click on PROCESSOR SETTINGS to view a screen like the following:

20.1.0.1 Basic Settings

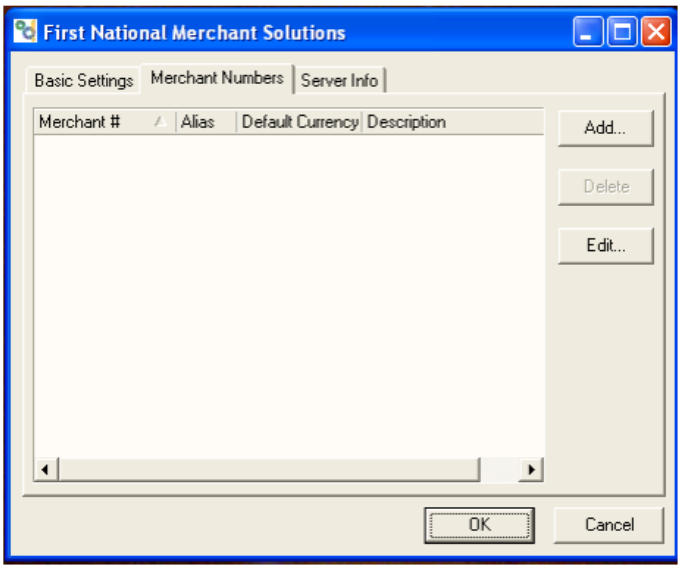
4. Click on the BASIC SETTINGS tab.

   BASIC SETTINGS information identifies the company presenting information to FNMS. In other words, it identifies the company that's running Trevance®.

   This is required information, which comes from FNMS.

20.1.0.2 Merchant Numbers

5. Click on the MERCHANT NUMBERS tab to view a screen like the following:



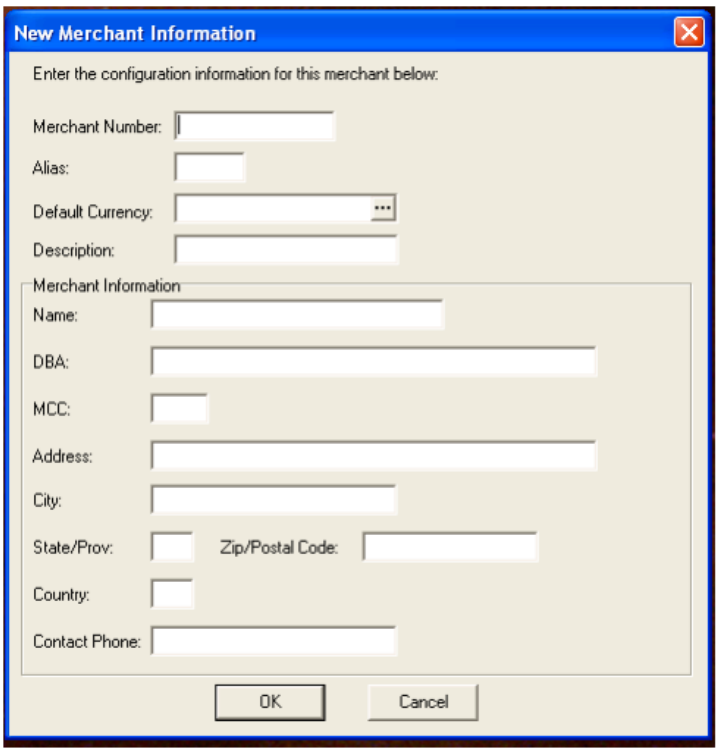
Merchant Numbers identify transactions as belonging to different categories, such as the different parts of a large company, mail order/phone order/web sales, or totally different companies (as in the case of an in-bound call center processing for many merchants).

Merchant Numbers are also used to process and report on transactions in different currencies. Although FNMS allows you to set the currency value with each and every transaction, it is typical, and considered a best practice, to have FNMS configure a Merchant Number for each currency in which you process.

You'll see the information in this screen again when you configure import files. At that time, the Merchant Number(s) and associated description(s) are automatically listed under the DEFAULT VALUES tab (in the MERCHANT NUMBER box).

The Merchant Number grid is sortable. Click on a heading (MERCHANT NUMBER, ALIAS, DEFAULT CURRENCY, DESCRIPTION) to change the sort order.

6. To add a Merchant Number, click on Add... to view:



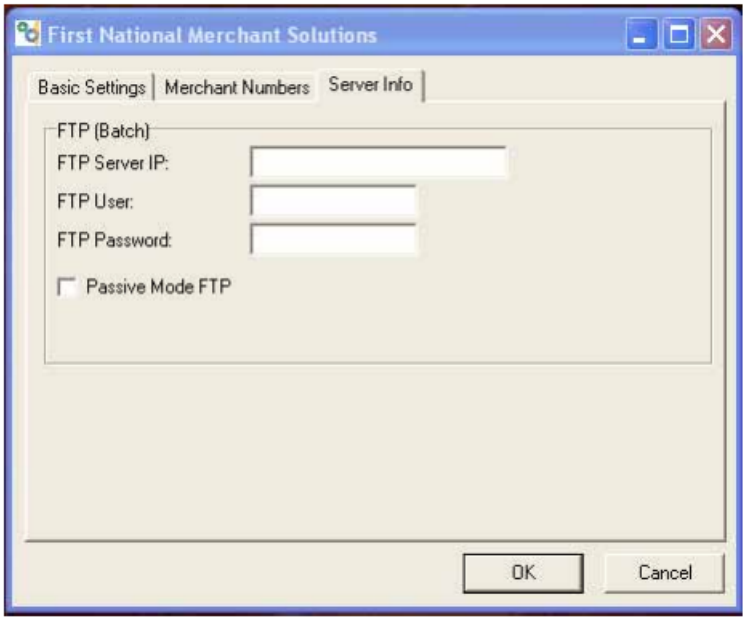
7. In the MERCHANT NUMBER field, type the value provided to you by FNMS.
8. The ALIAS field is provided for future functionality. Leave it blank for now.
9. Under Default Currency, click on ... to view a list of currencies.
10. Click on the currency you want. Trevance® automatically uses that currency for all transactions associated with that particular division ID.

    If you leave the field blank, U.S. dollars are used by default.
11. Enter a DESCRIPTION. This description is for your own use in identifying the submitter. The description is never sent to FNMS.
12. Enter the merchant information and location.

13. Click on OK

20.1.0.3 Server Info

14. Click on the SERVER INFO tab to view:



The server information helps set up communications with FNMS.

15. Fill in the boxes based on information you receive from FNMS.

16. Click on OK

20.2 Methods of Payment, Actions, and Required Fields

Trevance for FNMS supports the following methods of payment (MOPs):

- Credit card: American Express, Carte Blanche, Diners Club, Discover, JCB, MasterCard, Visa

- Purchase card (level II): American Express, MasterCard, Visa.
- Accounts Receivable check Conversion (ARC):
  - written
  - telephone
  - web

Trevance® automatically recognizes some of these methods of payment. For others, specific fields must be set. Refer to the "Method of Payment" documentation in the *Trevance Field Reference for FNMS* http:/auricsystems.com/tr_fnms_150

20.2.1 Required Information

Regardless of the method of payment, FNMS transactions require the following information:

- ACCOUNT: Credit card, debit card, or bank account number.
- ACTION: Authorization, sale, deposit, refund. Set to default or import with each transaction.
- AMOUNT
- MERCHANT NUMBER: Set to default or import with each transaction.
- MERCHANT ORDER NUMBER: Every transaction requires a merchant order number. This value is used for tracking transactions through FNMS and the Card Associations.

  Merchants should provide a MERCHANT ORDER NUMBER with each transaction. Trevance® generates an order number if one is not provided. If you're performing two-pass authorization transactions that are followed by deposits, you must use the same order number for the deposit and for the authorization. A unique order number for each transaction

helps reporting and reconciliation, but is not mandatory for FNMS.

- MERCHANT IDENTIFIER AND MERCHANT NAME: Configured in Trevance and never imported.

- TENDER TYPE Credit card, purchase card, check, etc. For some transactions—those using credit cards – there's no need to import the tender type. It is a good practice to always import the tender type so you are prepared for new future payment methods that may require the field. The following tables indicate when it's necessary to import the tender type.

The following tables show the minimum additional information that you must send for each method of payment—not the information that results in your best interchange rate (processing fee). These tables assume you're sending the ACCOUNT, ACTION, AMOUNT, and MERCHANT NUMBER.

Performing basic credit card and check processing with Trevance for FNMS is simple and can be set up quickly. Ask your FNMS representative what is necessary for more complicated transactions.

Table 20.1: Tsys - Credit Card

Authorization	*Deposit*	*Sale*	*Refund*
Expiration Date	Expiration Date	Expiration Date	Expiration Date
	Authorization Date		
	Authorization Code		

Transactions that contain the minimum information plus an expiration date are automatically identified as "credit card" transactions.

Sending a "C" in the TENDER TYPE field explicitly identifies credit card transactions.

Credit card account values can contain spaces or dashes ("-")..

Table 20.2: Tsys - Purchase Card (Level ll)

Authorization	*Deposit*	*Sale*	*Refund*
Expiration Date	Expiration Date	Expiration Date	Expiration Date

Continued on next page

Table 20.2 – *Continued from previous page*

Authorization	*Deposit*	*Sale*	*Refund*
Purchase Order	Purchase Order Number		
	Tax	Tax	
	Ship To Address (AM)	Ship To Address (AM)	
	Tender Type	Tender Type	
	Authorization Code		
	Authorization Date		

Purchase card (level II) transactions require the same minimum information as a credit card transactions, plus several additional fields.

American Express, MasterCard, and Visa accept level II transactions.

Purchase Card account values can contain spaces or dashes ("-").

You must explicitly identify Purchase Card transactions by importing "P" in the TENDER TYPE field.

You must provide the amount of tax, even if it is $0.00.

FNMS recommends providing the SHIP TO ADDRESS fields (ADDRESS, CITY, STATE, ZIP) for American Express (AM) purchase card transactions.

Table 20.3: Tsys - Accounts Receivable Check Conversion (ARC)

Authorization	*Deposit*	*Sale*	*Refund*
Routing Number	Routing Number	Routing Number	Routing Number
BillAddress: First Name	BillAddress: First Name	BillAddress: First Name	BillAddress: First Name
BillAddress: Last Name	BillAddress: Last Name	BillAddress: Last Name	BillAddress: Last Name
Check Number	Check Number	Check Number	Check Number
ECP Authorization Method [1]	ECP Authorization Method [1]	ECP Authorization Method [1]	ECP Authorization Method [1]
Checking Account Type [2]	Checking Account Type [2]	Checking Account Type [2]	Checking Account Type[2]
	Authorization Code		
	Authorization Date		

NOTES:

[1] Although FNMS allows merchants to set a default value for the ECP Authorization method, Trevance requires an "A" to be imported as the ECP Authorization Field; the "A" indicates that this is an "accounts receivable check conversion (ARC)" transaction.

[2] If the Checking Account Type field is not provided, Trevance® defaults to Consumer Checking

Trevance supports accounts receivable check conversion (ARC) transactions. The merchant is responsible for scanning the paper check and extracting the necessary information to submit to FNMS through Trevance®.

ARC is designed to improve check handling by turning paper checks into electronic transactions.

Trevance® automatically identifies ARC transactions as "check (tender type K)" transactions.

20.2.2 Generally Useful Fields

The following fields are generally useful for most types of transactions. Refer to the on-line field reference list for additional information.

- COMMENT (1 through 4): Four 128-character general-purpose fields. Not sent to FNMS. Use these for your own tracking purposes.
- CURRENCY: Usually set as a default at the merchant number level and not imported. Any imported value overrides the default.
- CUSTOMER IP ADDRESS: Useful for tracking and fraud purposes when processing e-commerce transactions.
- LAST ACTION SUCCEEDED: Returns "Y" whenever a requested transaction was successful. Otherwise, it returns "N." A useful first check to see if a transaction request was approved.
- RESPONSE CODE: FNMS's three-digit response code.

- SOFT DESCRIPTOR (1 and 2): Provides information on the cardholder's monthly statement. This must be set up at FNMS before you can use it.

In addition to the fields described above, you should also send the account holder's full name (FIRST NAME and LAST NAME fields) as well as the address, city, state, and ZIP or postal code whenever available. This helps reduce your interchange rate (processing fee). If you do not have a full address, at least obtain and send a ZIP code (U.S.) or postal code (Canada and United Kingdom).

Additionally, obtain and transmit the card security code (CVV2/CID) information with authorizations.

Your First National Merchant Solutions representative can help you choose what set of fields best fits your requirements.

20.3 Advanced Transaction Configuration

The preceding tables showed the basic transaction information for each type of transaction. Once you get beyond the basics, you must consult with your FNMS representative to determine what data you should be sending for maximum efficiency and lowest processing fees (also called interchange).

FNMS's textitBatch and Direct Settlement Specifications describe over 100 possible fields that can be transmitted. The specific fields you should send will depend on your market type, your business class (ecommerce, MOTO, recurring, IVR, etc.), and the forms of payment you accept (credit card, purchase card, check, ARC, etc.). Working with your FNMS representative is the quickest way to determine which fields you should send.

20.4 Generating an SSH Key

Tsys requires a 2048-bit RSA key. Unfortunately, there are several slightly different variants on the format and the keys generated directly by Trevance® are not acceptable by Tsys. If you have a Linux or Unix box available, ASI recommends you use openSSH to generate your key. If this is not accessible to you, please contact Auric for additional options.

20.4.1 Generating 2048-bit RSA key with OpenSSH

These instructions are for Linux, Unix, & Mac OS X:

1. Use ssh-keygen to create a 2048-bit rsa key:
   ssh-keygen -t rsa -b 2048 -f trevance
   t (type)
   b (bits)
   f (filename)
2. When prompted, enter a passphrase for the new key. *Auric Systems strongly recommends using a passphrase.*
3. Key generation is now complete. Note the names of the private and public key files. Your private key is saved in trevance. Your public key is saved in trevance.pub.
4. Send the public key to Tsys so that it can be installed on their SSH server. In this example, the public key is named trevance.pub.
5. Import the private key into Trevance®. Launch the console and pause the server if it is running.
6. Select Configure/Processor Settings. Choose the Server Info table.
7. Click the Import Private Key button.

8. Enter the path to the private key file you generated in Step 1. Also, enter the passphrase you used when generating the key.

Import Private Key File
Import an externally-generated SSH private key file. Specify the password used to encrypt the key file when it was generated (if one was used). Provide the matching public key file to your payment processor so that this key can be used for authentication.
Private Key File:
Browse ...
Private Key File Password:
OK
Cancel

9. Click "OK". You should see the following message:
10. You've now successfully created a key pair and imported the private key into Trevance®.

Part IV

PA DSS Secure Implementation Guide

1 Do Not Retain Full Magnetic Stripe or CVV2 Data

1.1 General

- The Trevance® and CN!Express® real-time web interfaces accept transactions containing CVV2/CID, magnetic stripe, and debit card PIN block data. This information is transmitted directly to the processor and never stored.
- The Trevance® and CN!Express® batch file interfaces accept transactions with CVV2/CID data. This feature is provided for integration with legacy systems. Auric recommends that CVV2 data not be transmitted in files.
- Import and export file encryption formats are discussed later in this document.
- If you do not encrypt the import file, Auric strongly recommends you multi-pass delete the import file after it is read.
- If you do not delete the import file, Auric strongly recommends you mask sensitive data after import. In this mode, instead of just changing the imported file's extension from .IMP to .DNE, CN!Express® copies the .IMP file to a temporary file while masking sensitive data such as account number and CVV2/CID. When the copy is complete, the .IMP file is deleted and the new, masked, copy is given the .DNE extension.
- Do not export the account code. Instead, use the order number field or an internal tracking ID in one of the four comment fields.
- Never send sensitive customer information to Auric for support or any other reason.

- Sensitive authentication data should be collected only when needed to solve a specific problem.
- Any such sensitive data collected must be stored in a secure manner, in specific known locations, and with limited access.
- Collect only the limited amount of data required to solve a problem.
- Securely delete any such sensitive collected data immediately after use.

1.2 Trevance®

1.2.1 Securely Delete Files

Trevance® supports the ability to perform multi-pass file overwrites and deletion. After a batch file is imported, it is deleted in a secure manner by being overwritten multiple times before the actual deletion. If this should cause excessive hard drive activity in your specific installation, the second-best approach is to use the One-Pass Overwrite and Delete. See section 3.8.2 Selecting a Secure File Deletion Method.

You must remove historic data (such as old databases and database backups no longer being used) using a secure removal tool such as SDelete for Windows.

- *Configure/Options Security Tab*
- *Multi-Pass Overwrite and Delete* is checked.
- *Configure/Batch Files/Imports* Dialog
  - *CVV/CID* field is not imported.
- *After Import* Tab
  - *Delete File*

- *Encryption* Tab
  - *Import Files are Encrypted* is checked.
  - *Export Files are Encrypted* (optional, better to not export sensitive data).

1.2.2 Proper Log Handling

Run those logs appropriate for the environment. Ensure log masking is active.

Note: Trevance® and CN!Express® can only mask information appearing in the proper field. If a credit card or CVV2 value should be placed in the wrong field, the software has no way to know it should be masked.

- From the *Configure/Options Troubleshooting* Tab:
  - Turn off all *Additional Logs* that you are not explicitly using.
  - If you do turn on any Additional Logs, check the *Mask Identifying Information in Log Files* checkbox. This causes the sensitive data such as account numbers and CVV2/CID values to be masked in the output streams.

1.2.3 Do Not Store CVV2 Field

CVV2 data should never be transmitted in batch files.

- From the *Configure/Batch Files/Imports* dialog, check the following:
  - *CVV/CID* field is not imported.
- *Configure/BatchFiles/Exports* dialog
  - *Account* field is not exported, or exported masked.

1.3 CN!Express®

1.3.1 Securely Delete Files

CN!Express® supports the ability to perform multi-pass file overwrites and deletion. After a batch file is imported, it is deleted in a secure manner by being overwritten multiple times before the actual deletion. If this should cause excessive hard drive activity in your specific installation, the second-best approach is to use the One-Pass Overwrite and Delete. See Appendix C Secure File Deletion for details.

You must remove historic data (such as old databases and database backups no longer being used, using a secure removal tool such as SDelete for Windows.

- *File Formats* Tab
  - Set *After Importing a File to Multi-Pass Overwrite and Delete*. After a batch file is imported it is deleted in a secure manner by being overwritten multiple times before the actual deletion.
- *Files Tab*
  - *Decrypt Files Before Import* is checked.
  - *Encrypt Files Before Export* is checked (optional, better to not export sensitive data).

1.3.2 Proper Log Handling

Run those logs appropriate for the environment. Ensure log masking is active.

- From the *Advanced Tab*

  - Turn off all *Optional Logs* that you are not explicitly using.

1.3.3 Do Not Store CVV2 Field

CVV2 data should never be transmitted in batch files.

- From the *File Formats Tab, Edit Format...* buttons (one for Import one for Export)
  - CVV/CID field is not imported or exported.
  - Account field is not exported, or exported masked.

1.4 PaymentVault™

1.4.1 Securely Delete Files

Not applicable since PaymentVault™ does not import files.

1.4.2 Proper Log Handling

PaymentVault™ logs have no card holder data in them.

1.4.3 Do Not Store CVV2 Field

PaymentVault™ does not handle CVV or unencrypted account data.

2 Protect Stored Cardholder Data

2.1 General

- Trevance® and CN!Express® support external Key Management Systems
- Merchants should develop a cardholder data retention policy.
- Card holder data exceeding the defined retention policy retention period must be purged.
- Credit card data is never displayed by Trevance®, CN!Express®, or PaymentVault™.
- All logs, including debug logs, mask sensitive data fields.
- When Trevance® and CN!Express® using the embedded database are uninstalled, the uninstall routine securely deletes the data files in order to ensure locally encrypted data is removed securely.
- When uninstalling Trevance®, CN!Express®, or PaymentVault™ all cryptographic material must be removed. The only cryptographic material is the encrypted card holder accounts that may be in the database or backup files.
- Customers are advised that Windows restore points; backups; crash files; debug files and any other type of file, that takes a snapshot of the registry and/or hard drive where Trevance®, CN!Express®, or PaymentVault™ is loaded (whether resident on the system or not) must be deleted using the secure delete process described in this document for the customer to maintain PCI compliance.
- Use a secure deletion program, such as SDelete, to remove these files.
- Removal of historic cryptographic material is absolutely necessary for PCI DSS compliance.

- Trevance® and CN!Express® require the use of an external key server application or service (Key Service).
- The Key Service must:
  - be PCI compliant.
  - rotate keys at least once every 12 months.
  - use strong encryption (such as 256-bit AES encryption)

2.2 Trevance®

- Configure/External Key Manager
- Select the Key Management software/service to which you will connect.
- Enter the proper credentials.
- Encryption keys for all sensitive data are now managed externally.
- Trevance® Stores Encrypted Cardholder Information:
- In embedded Firebird database contained in the Data subfolder under the default installation directory.
- Or, in the remotely-installed Firebird database. Data locations should be listed and noted.
- In backup (gbk) files. Note the location as set in the Trevance® Configuration utility.
- If using the local embedded Firebird database, then securely delete the database file: PROD.FDB. Also delete the backup files: cnxap_[The Date].GBK.
- If using the remote Firebird database, you must delete the CN!Express® schema from the remote Firebird installation and remote files in a manner compliant with your PCI policies and procedures. Such removal is absolutely necessary for PCI DSS compliance.
- After the update from Trevance® 2.x to 3.0 Trevance® will immediately start using the new Key Manager based keys

for all existing sensitive cardholder data. Transitory information (such as transactions held for end of day settlement and cached PaymentVault™ data) will continue to use the old key. Such data is transitory and will be flushed from the system within a few hours (transactions queued for end of day) or days (PaymentVault™ data is cached depending on the number of days you have configured to hold it in Trevance®).

- If you are using PaymentVault™, Trevance® will re-encrypt the historic data as it is retrieved from PaymentVault™ during normal UTID retrieval.

2.2.1 Clearing Sensitive Data

Trevance® supports sending batch authorization transactions. Authorization transactions may include sensitive cardholder data (CVV or CID). Because these are batch transactions, it is necessary for Trevance® to temporarily store this information in its internal database as the batch is prepared for transmission to the payment processor.

To ensure that this data is not retained any longer than necessary, Trevance® clears this information from its database when the batch export file is generated (Trevance® also never exports this information).

On a general level, batch transmission through Trevance® works like this:

1. Merchant places a delimited-text file with batch transactions in the Trevance® import directory.
2. Trevance® reads in and parses this file, storing the information in its internal database.
3. Trevance® uses this stored information to create a file in the proper format for the payment processor.

4. Trevance® uploads the processor file to the processor.
5. Trevance® downloads the processor response file when it is available.
6. Trevance® creates an export file which includes a line for each transaction that was imported. The information in the export line may be a combination of items that are stored in the database as imported and responses that are returned from the payment processor.

The process may be interrupted at any point and resumed if Trevance® is paused or restarted. Also, batches may be "re-queued" for transmission if the payment processor requests that a file be re-sent. This requires that Trevance® retain all imported information until each step in the process is complete.

When the export file is generated (step 6), Trevance® clears CVV information from its database as soon as the export is complete. This is done through a database update statement which is always executed as part of the transaction which updates the database following the export. This ensures that sensitive information is not stored in the database after batch processing is complete.

2.2.2 Key Handling During Upgrade from Trevance® 2.x to Trevance® 3.x

Trevance® 3.0 requires an external key manager to track encryption keys. Encryption is used in Trevance® to secure cardholder data and other sensitive information (such as payment processor account passwords). Using an external key manager allows Trevance® to use several different keys to encrypt data, making compromise of the entire data set much more difficult for attackers.

In Trevance® 2.0, there were two internal encryption keys that were generated at the merchant site when the merchant entered

the server passphrase. One key was used for cardholder data, and the other for administrative passwords. These keys were then encrypted using the passphrase, which was to be entered in two segments by two administrators. The passphrase was in turn encrypted using Windows encryption (DPAPI) so that it could be stored and would not need to be re-entered each time the system was restarted.

Key manager encryption improves on passphrase encryption in two ways:

1. There are more keys than the two which had been used in previous versions of Trevance® and
2. Users do not need to track a passphrase for the Trevance® server, and the server may be migrated from physical machine to physical machine without needing to recover the data (as long as connection to the same key server is maintained).

When upgrading from Trevance® 2.x to Trevance® 3.0, Trevance® must retain the existing keys so that it can decrypt any existing data that may be stored in the database at the time of the upgrade (or stored in a Payment Vault server). To do so, it removes the passphrase encryption from these keys and re-encrypts them using a key delivered by the key manager. This takes passphrase encryption out of the process but saves the keys that may be required to decrypt existing data.

At startup, Trevance® 3.0:

1. Checks to see if a legacy key was set.
2. If it has been set, checks to see if it was in the "old" (passphrase) or "new" (key-manager) format.
3. If it is in old format, Trevance® requires that a key manager be configured or startup or it cannot continue (a key manager is not required for demo mode, so it is possible that

Trevance® would be in this state if upgrading from demo mode).

4. Attempts to decrypt the old-format keys using the passphrase. If the passphrase cannot be recovered (because, for example, Trevance® had been moved to another machine) then Trevance® requires that the merchant enter the two-segment passphrase at this point. The passphrase is checked against a hash to make sure that the passphrase is correct.
5. Requests a current key from the key manager.
6. Uses the key manager key to encrypt the two legacy keys.

Data that has been encrypted by a key manager key is "tagged" with the key version, so these are easily differentiated from data encrypted by legacy keys, which are not tagged. When Trevance® reads an encrypted, but untagged data item, the appropriate legacy key is used for decryption.

2.3 CN!Express®

- External Key Manager Tab
- Select the Key Management software/service to which you will connect.
- Enter the proper credentials.
- Encryption keys for all sensitive data are now managed externally.
- CN!Express® Stores Encrypted Cardholder Information:
- In embedded Firebird database contained in the Data subfolder under the default installation directory.
- Or, in the remotely-installed Firebird database. Data locations should be listed and noted.
- In backup (gbk) files. Note the location as set in the Trevance® Configuration utility. Backup files are generated only for the embedded solution.

- If using the local embedded Firebird database, then securely delete the database file: CNXAP.FDB. Also delete the backup files: cnxap_[The Date].GBK.
- If using the remote Firebird database, you must delete the CN!Express® schema from the remote Firebird installation and remote files in a manner compliant with your PCI policies and procedures. Such removal is absolutely necessary for PCI DSS compliance.
- After the update from CN!Express® 4.x to 5.0 CN!Express® will immediately start using the new Key Manager based keys for all existing sensitive cardholder data. Transitory information (such as transactions held for end of day settlement and cached PaymentVault™ data) will continue to use the old key. Such data is transitory and will be flushed from the system within a few hours (transactions queued for end of day) or days (PaymentVault™ data is cached depending on the number of days you have configured to hold it in Trevance®).
- If you are using PaymentVault™ CN!Express® will re-encrypt the historic data as it is retrieved from PaymentVault™ during normal UTID retrieval.

2.3.1 Clearing Sensitive Cardholder Data in Batch Transactions

CN!Express® supports sending batch authorization transactions. Authorization transactions may include sensitive cardholder data (CVV or CID). Because these are batch transactions, it is necessary for CN!Express® to temporarily store this information in its internal database as the batch is prepared for transmission to the payment processor.

To ensure that this data is not retained any longer than necessary, CN!Express® clears this information from its database when

the batch export file is generated (CN!Express® also never exports this information).

On a general level, batch transmission through CN!Express® works like this:

1. Merchant places a delimited-text file with batch transactions in the CN!Express® import directory.
2. CN!Express® reads in and parses this file, storing the information in its internal database. For single-item files, CN!Express® does not store the information at all, but directly submits the transaction to the processor.
3. CN!Express® submits each item in the batch as an individual, on-line transaction, and updates its database with processor responses when these are received. Multiple transactions may be submitted simultaneously.
4. When CN!Express® has received all of the responses for a batch, it reads the information out of the database for each transaction and builds and exports a delimited-text file.

CN!Express® clears the CVV from its internal storage as soon as the response is received from the processor (step 3 above). In the database, each transaction is stored as an "object," so updating a transaction with responses actually requires replacing that transaction in the database with a new one. As soon as the response is received, CN!Express® clears the CVV from the transaction object along with writing the processor responses to it. It then overwrites the transaction in the database with the new one, eliminating CVV from storage.

2.3.2 Key Handling During Upgrade from CN!Express® 4.x to CN!Express® 5.x

CN!Express® 5.0 introduces support for external key managers to track encryption keys. Encryption is used in CN!Express® to

secure cardholder data and other sensitive information (such as payment processor account passwords). Using an external key manager allows CN!Express® to use several different keys to encrypt data, making compromise of the entire data set much more difficult for attackers.

In CN!Express® 4.0, there was a single encryption key that was generated at the merchant site when the merchant entered the server passphrase during configuration. The key was then encrypted using the passphrase, which was to be entered in two segments by two administrators. The passphrase was in turn encrypted using Windows encryption (DPAPI) so that it could be stored and would not need to be re-entered each time the system was restarted.

This key was used for cardholder data and for encrypting the keys for external file encryption. Administrative data was encrypted by the configuration program using Windows encryption.

Key manager encryption improves on passphrase encryption in two ways:

1. there are now multiple keys
2. users do not need to track a passphrase for the CN!Express® server, and the server may be migrated from physical machine to physical machine without needing to recover the data (as long as connection to the same key server is maintained).

CN!Express® 5.0 uses key-server keys for both cardholder and administrative data, so Windows encryption is no longer required.

When upgrading from CN!Express® 4.x to CN!Express® 5.0, CN!Express® must retain the existing key so that it can decrypt any existing data that may be stored in the database at the time of the upgrade (or stored in a Payment Vault server). To do so, it removes the passphrase encryption from these keys and re-

encrypts them using a key delivered by the key manager. This takes passphrase encryption out of the process but saves the keys that may be required to decrypt existing data.

At startup, CN!Express® 5.0:

1. Checks to see if a legacy key was set.
2. If it has been set, checks to see if it was in the "old" (passphrase) or "new" (key-manager) format.
3. If it is in old format, CN!Express® requires that a key manager be configured or startup cannot continue (a key manager is not required for demo mode, so it is possible that CN!Express® would be in this state if upgrading from demo mode).
4. Attempts to decrypt the old-format keys using the passphrase.
5. Requests a current key from the key manager.
6. Uses the key manager key to encrypt the legacy key.

Data that has been encrypted by a key manager key is "tagged" with the key version, so these are easily differentiated from data encrypted by legacy keys, which are not tagged. When CN!Express® reads an encrypted, but untagged data item, the appropriate legacy key is used for decryption.

The configuration utility for CN!Express® also makes a connection to the external key manager. The configuration utility retains the ability to read Windows-encrypted or passphrase-encrypted configuration files, but it always writes new configurations using managed keys.

2.4 PaymentVault™

PaymentVault™ stores encrypted data, but does not use encryption.

- PaymentVault™ Stores Encrypted Cardholder Information:
- In configured PostgreSQL database.
- Optionally in configured Firebird database. Also in Firebird backup files if running with the embedded Firebird database.
- If using the local embedded Firebird database, then securely delete the database file: PV.FDB
- If using the PostgreSQL database, you must delete the PaymentVault™ schema from the PostgreSQL installation and remove the files in a manner compliant with your PCI policies and procedures. Such removal is absolutely necessary for PCI DSS compliance.

2.4.1 Re-Encrypting Historic Data

As historic data is retrieved from PaymentVault™, Trevance®, and CN!Express® examine the key that was used to encrypt that data. If the key is not the current key, Trevance® and CN!Express® re-encrypt that value and write it back to PaymentVault™. This converts your data encrypted with historic keys to data encrypted with the current key.

3 Secure Authentication Features

3.1 General

You must maintain secure authentication for access to all payment processing applications and servers.

- Unique user IDs must be used for all administrative access to Trevance®, CN!Express®, and PaymentVault™.
- All Trevance®, CN!Express®, and PaymentVault™ administration must occur on the server running the payment application.
- You must maintain PCI DSS compliant access and logins to the servers on which Trevance®, CN!Express®, and PaymentVault™ are installed.
- Trevance® and CN!Express® provide default accounts that must be replaced before running either program in Test or Production modes.
- Trevance® and CN!Express® passwords may be as long as 40 characters. This encourages the use of long, easily remembered passwords (sentences, poems, etc.) vs. short cryptic passwords. Spaces and punctuation are acceptable password characters.
- Trevance® and CN!Express® maintain a history of the last four passwords used and do not allow them to be reused.
- Passwords must be maintained according to company policies and procedures. Specifically, PCI recommends that passwords be changed every 90 days.
- You must not use administrative accounts for payment application logins (e.g., don't use the "sa" account for payment application access to the database).

- You must assign secure authentication default accounts (even if they won't be used), and then disable or do not use the accounts.
- You must assign secure authentication for payment applications and systems whenever possible.
- You must create PCI DSS compliant secure authentication to access the payment application, per PCI DSS Requirements 8.5.8 through 8.5.15.
- Changing "out of the box" installation settings for unique usernames and secure authentication will result in non-compliance with PCI DSS.

3.2 Trevance®

3.2.1 Replace Default Users

From the Configure/Administer Users dialog:

- Create a new user.
- Set the User Type to Administrator.
- Enter a strong password consisting of at least seven (7) characters and both alpha and numerical characters.
- Repeat for default WEB User. (Trevance® CN-3500 does not have a WEB User since it does not have a web interface.)
- Create a unique user ID for each person requiring access to the Trevance® console.
- Delete the original Admin user.
- Delete the original WEB user.

Provide Administrative access only to those users who must change Trevance® configurations. All other users should receive Console access.

If a Trevance® user fails to log in to the Console after six attempts, they are locked out of the system for 30 minutes. The one exception to this is the WEB user accounts for the real-time web transaction interface. A lockout in this instance would lead to a denial of service.

Trevance® Administrative accounts are automatically logged-out after 15 minutes of inactivity. Console users are not automatically logged out since typically these are used as long-term monitoring accounts.

Auric recommends that Trevance® Administrative accounts be used solely for administration, and not for monitoring purposes.

3.3 CN!Express®

3.3.1 Replace Default Users

From the Configure/Administrator Users dialog:

- Create a new user.
- Set the User Type to Web Service or Web Console.
- Click the Manager checkbox to give Web Console users access to ability to pause/resume CN!Express® or reload redo logs.
- Enter a strong password of at least seven (7) characters and both alpha and numeric characters.
- Create a uinque user ID for each person requiring access to the CN!Express® console.

Provide Manager access only to those users who must manage/control CN!Express® remotely.

If a Manager fails to log in after six attempts they are locked out of the system for 30 minutes. The exception to this is the WEB user accounts for the real-time web transaction interface. A lock out in this instance would lead to a denial of service.

Manager accounts are automatically logged out after 15 minutes of inactivity. Non-managers users are not automatically logged out since typically they are doing long-term monitoring.

Auric recommends that Manager accounts be used solely for starting/stopping CN!Express® remotely, and not for monitoring purposes.

3.4 PaymentVault™

All access to PaymentVault™ is via Trevance® or CN!Express®. Access to the PaymentVault™ server is tied to the IP addresses listed in PaymentVault™.

4 Log Payment Application Activity

4.1 General

Trevance® and CN!Express® maintain a running log of Administrative, Manager, and Console users who connect. This log should be regularly monitored for failed log-in attempts.

- Use a Network Time Protocol service to ensure the time on the Trevance®, CN!Express®, and PaymentVault™ servers is properly synchronized.
- Check the timezone and Daylight Savings/Standard Time flag is set properly on the servers.
- Check all logs on a daily basis.
- Implement automated audit trails to reconstruct the following events for all system components:
  - All individual user access to cardholder data.
  - All access to audit trails.
  - All actions taken by any individual with root or administrative privileges.
  - Access to all audit trails.
  - Invalid logical access attempts.
  - Use of identification and authentication mechanisms.
  - Initialization of the audit logs.
  - Creation and deletion of system-level objects.
- Record at least the following audit trail entries for each event for all system components:
  - User identification
  - Type of event
  - Date and time

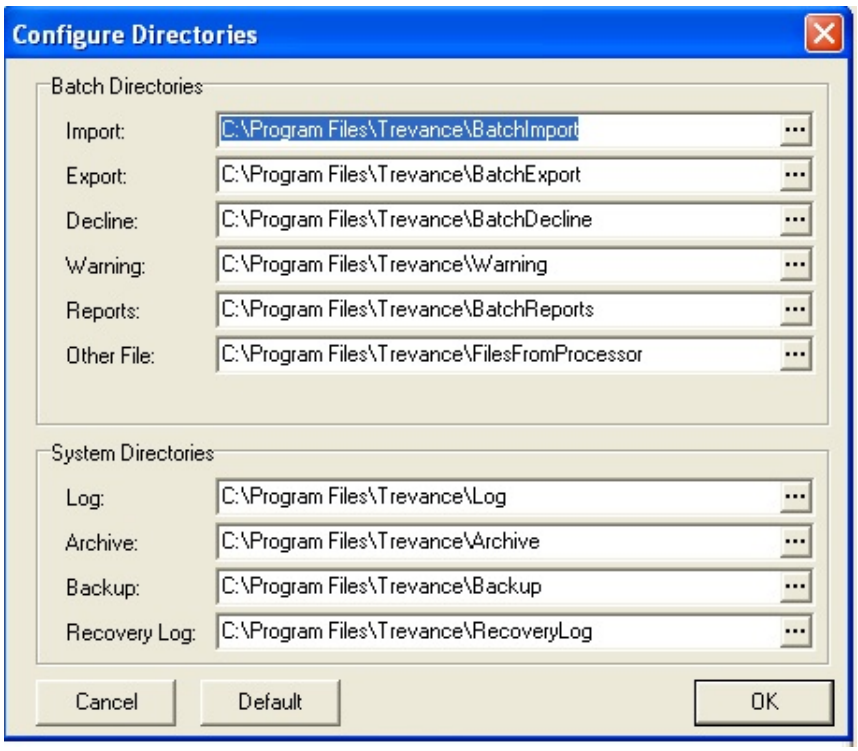
  - Success or failure indication
  - Origination of event
  - Identity or name of affected data, system component, or resource.

- Trevance® and CN!Express® have audit logs that are always active.
- You must capture and store these logs for at least one year to maintain PCI compliance. Disabling logs will result in non-compliance with PCI DSS.
- Any attempt to disable these logs will result in non-compliance with PCI DSS.

4.2 Trevance®

PCI compliance requires that the following Trevance® logs be stored for a year. Auric Systems International recommends forwarding these logs to a central repository.

- The audit log (audit_YYYYMMDD.log) contains a list of activities performed by Administrative and Console users. This log contains both the user's log-in name and a date/time stamp at which the activity occurred.
- The console user log (console_user_YYYYMMDD.log) shows console log-in actions. This log contains a date/time stamp, a log-in success/failure message for a specific user, and the IP address from which that user attempted to log in.
- The Trevance® log (trevance_YYYYMMDD.log) shows general application activity. This log contains a date/time stamp along with the specific action occurring within Trevance®. Log entries show both informative process as well as error messages.



From the Configure/Directories dialog:

- Ensure the Log field is pointing to a valid disk location. This is the directory that will contain all your logs.

The Trevance® log directory contains a number of logs. The three that you should forward to a centralized logging location are:

- audit_YYYYMMDD.log
- console__user_YYYYMMDD.log
- Trevance_YYYYMMDD.log

From the Configure/E-Mail Notification dialog:

- check *All Logs* to have the daily logs automatically emailed to you.

- configure the settings for your SMTP mail server.

- select a time at which the logs should be emailed to you.

- check *Login Report* to receive an email whenever anyone logs into Trevance®.

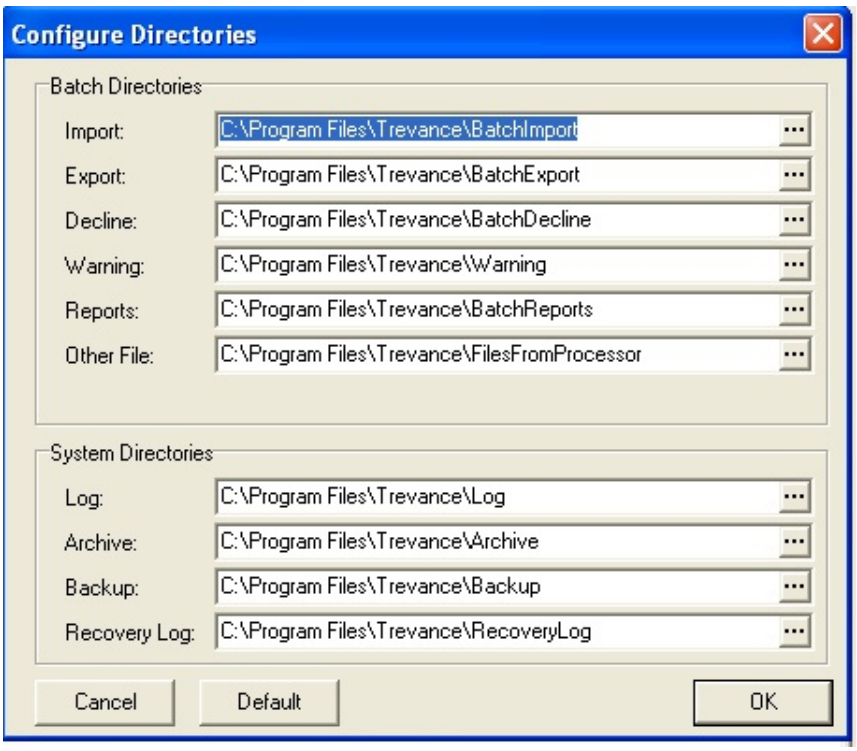
4.3 CN!Express®

The audit log provides a list of activities performed by the Manager using the web administrative interface. Console users can only Monitor CN!Express® activity. This log contains both the users log-in name and a date/time stamp at which the activity occurred.

The console user log maintains a running log of Manager and Console users who connect to CN!Express®via the web administrative interface. This log should be regularly monitored for failed log-in attempts.

The cnxap.log file shows general application activity. This log contains a date/time stamp along with the specific action occurring within CN!Express®. Log entries show both informative process as well as error messages.

These logs are stored as simple text files that are easily reviewed.



The CN!Express® log directory contains a number of logs. The three that you should forward to a centralized logging location are:

- audit_YYYYMMDD.log
- console__user_YYYYMMDD.log
- cnxap_YYYYMMDD.log

From the Advanced directory in the CN!Express® Configuration utility:

- Ensure the Log Directory field is pointing to a valid disk location. This is the directory that will contain all your log files.

The CN!Express® From the Configure/E-Mail Notification dialog:

- check All Logs to have the daily logs automatically emailed to you.
- configure the settings for your SMTP mail server.
- select a time at which the logs should be emailed to you.
- check Login Report to receive an email whenever anyone logs into CN!Express®.

4.4 PaymentVault™

These PaymentVault™ logs logs may be useful for evaluating PaymentVault™.

- PaymentVault™ never contains sensitive cardholder information (the transactions have been sanitized).
- A new log is created each day. The actual name of the log will contain the date as well as the base name (e.g., PV 20110914.log).
- PaymentVault™ Log: Contains the general activity of the PaymentVault application/service.
- Audit Log: Lists external access to the PaymentVault Server

5 Develop Secure Payment Applications

5.1 General

This section of the PA-DSS standard is heavily focused on the development of secure web (public Internet-accessible) applications.

Although Trevance®, CN!Express®, and PaymentVault™ have web interfaces, it is not a web application and is not designed to be implemented directly on the public Internet. Trevance®, CN!Express®, and PaymentVault™ are designed for use only on internal networks. See Section 8 below for recommendations on secure network implementation.

Where applicable, Auric Systems International follows the Open Web Application Security Project (OWASP) guidelines available at http://www.owasp.org. Auric Systems International recommends anyone integrating payment processing into their web site also follow the OWASP guidelines.

6 Protect Wireless Transmissions

6.1 General

Trevance®, CN!Express®, and PaymentVault™ implementations neither require nor recommend the use of wireless networking.

If Trevance®, CN!Express®, or PaymentVault™ is integrated into a system using wireless payment applications, you must address the PCI compliance requirements including:

- Install perimeter firewalls between any wireless networks and the cardholder data environment, and such firewalls must deny or control any traffic from the wireless environment into the cardholder data environment.
- Change wireless vendor defaults including but not limited to keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.
- Use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication transmission. For all new wireless implementations, it is prohibited to implement WEP if wireless networks are used in the Customers payment environment after March 31, 2009 and remove WEP completely by June 30, 2010.
- Proper key rotation
- Removal of all default keys from wireless equipment

7 Test Payment Applications to Address Vulnerabilities

7.1 General

In addition to on-going internal testing Auric Systems International monitors outside security sources and product-specific mailing lists to check for product vulnerabilities. If a vulnerability is found in the Trevance®, CN!Express®, or PaymentVault™ system, you will be so informed via a security alert and a timely correction will be provided.

8 Facilitate Secure Network Implementation

8.1 General

Figure 8.1 shows Trevance®, CN!Express®, and PaymentVault™ implemented in a secure network configuration.

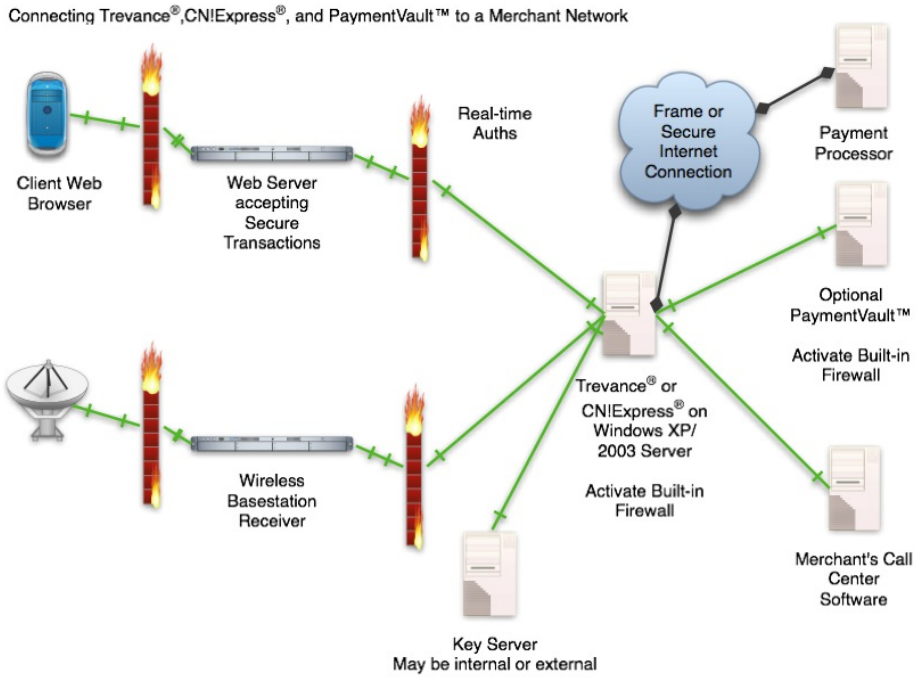


Figure 8.1: Network Installation

- Operate Trevance®, CN!Express®, and PaymentVault™ on their own, separate servers.

- Isolate the Trevance®, CN!Express®, and PaymentVault™ servers from the public Internet.
- Maintain your web server in a DMZ as shown in the diagram.
- Do not run Trevance®, CN!Express®, and PaymentVault™ in the DMZ (where the Web Server or Wireless Application Server are shown in the diagram).
- If your application must use wireless, provide wireless access through a separate firewall and isolate the application server.

9 Cardholder Data Must Never Be Stored on a Server Connected To the Internet

9.1 General

Trevance®, CN!Express®, and PaymentVault™ run on the local, private network and not in either the DMZ or on a server directly connected to the Internet.

You must never store cardholder data on Internet-accessible systems (e.g., web server and database server must not be on same server).

10 Facilitate Secure Remote Software Updates

10.1 General

Auric does not force automatic Trevance®, CN!Express®, or PaymentVault™ updates.

- The latest updates for Trevance® and CN!Express® are always available for immediate download from the Auric Systems International web site at http://www.AuricSystems.com/.
- PaymentVault™ updates are released privately as necessary.
- Both MD5 and SHA-256 hashes are provided on the Auric Systems International web site.
- After downloading the release or update, you should perform your own MD5 and/or SHA-256 calculation on the downloaded file to check the hashes before installing. For additional security, these hashes are also available via email from Auric Systems International. Please call tech support for details. Auric Systems International provides tools to perform these calculations, but recommends you use third-party tools to ensure integrity.

11 Facilitate Secure Remote Access to Payment Application

11.1 General

- Auric does not have remote access to the system where Trevance®, CN!Express®, or PaymentVault™ is installed.
- Whenever accessing the system where Trevance®, CN!Express®, or PaymentVault™ is installed, you must use two-factor authentication (i.e., username and password plus an additional authentication item such as a token or certificate).
- Any integrator that has remote access to the system where Trevance®, CN!Express®, or PaymentVault™ is installed must use and implement remote access software security procedures. For example:
  - Change default settings in the remote access software (for example, change default Passwords and use unique Passwords for each customer).
  - Allow connections only from specific (known) IP/MAC addresses.
  - Use strong authentication or complex Passwords for logins.
  - Enable encrypted data transmission.
  - Enable account lockout after a certain number of failed login attempts.
  - Configure the system so a remote user must establish a Virtual Private Network ("VPN") connection via a firewall before access is allowed.
  - Enable the logging function.
  - Restrict access to customer Passwords to authorized reseller/integrator personnel.

- Establish customer Passwords according to PCI DSS requirements 8.1, 8.2, 8.4, and 8.5.

11.2 Trevance®

Use of the Trevance® Console is restricted to administrators logged into the same computer running Trevance®.

Trevance® may be monitored, but not administered remotely via the Trevance® Console.

The Trevance® Console is for use within your corporate network. Never provide access from the Internet to the Remote Console.

Credit card information is not accessible via the Remote Console.

11.3 CN!Express®

All remote access to the CN!Express® server is via the CN!Express® Web Console.

CN!Express® supports HTTPS connections to the Web Console. This console is for use within your corporate network. Never provide access from the Internet to the Web Console.

Credit card information is not accessible via the Web Console.

11.4 PaymentVault™

PaymentVault™ does not provide a remote monitoring system.

12 Encrypt Sensitive Traffic Over Public Networks

12.1 General

- Trevance®, CN!Express®, and PaymentVault™ are designed for installation on a private network – not a public network. As such, sensitive traffic is not communicated over the public network.
- Trevance®, CN!Express®, and PaymentVault™ have no facility for emailing credit card information.
- Never email sensitive credit card information in an unencrypted form.
- If you should transmit any cardholder data over the public Internet, you must use secure encryption transmission technology (for example, IPSEC, VPN, SSH, or SSL/TLS).

12.2 Trevance®

Trevance® sends transactions to payment processor systems via secure VPN or leased-line connections as defined by the payment processors.

12.3 CN!Express®

CN!Express® sends transactions to payment processor gateways using secure HTTPS protocols as defined by the specific gateway provider.

12.4 PaymentVault™

PaymentVault™ communicates only with Trevance® and CN!Express® via the local private network.

13 Encrypt all Non-Console Administrative Access

13.1 General

13.2 Trevance®

- All administrative access to Trevance is through the Trevance Console.
- All configuration changes must occur through the Trevance Console.
- All Administrative changes must occur from a Trevance Console running on the same server as Trevance.
- Access to the Trevance Console is managed by operation-system level user permissions.
- All non-console administrative access to the Trevance® system (via Windows Remote Desktop or other remote access methods) must employ secure authentication and strong encryption to prevent the compromise of administrative credentials or sensitive data. For example, if Windows Remote Desktop access is used, it must be configured to require strong encryption (minimum of 128-bit key). Refer to this Microsoft TechNet article for an example: http://technet.microsoft.com/en-us/library/cc770833.aspx.

13.3 CN!Express®

- All administrative access to CN!Express is through the CN!Express Settings Manager which must be run on the same machine as CN!Express.

- Access to the Settings Manager is maintained by operating-system level user permissions.
- All configuration changes must occur through the CN!Express Settings Manager
- All non-console administrative access to the CN!Express® system (via Windows Remote Desktop or other remote access methods) must employ secure authentication and strong encryption to prevent the compromise of administrative credentials or sensitive data. For example, if Windows Remote Desktop access is used, it must be configured to require strong encryption (minimum of 128-bit key). Refer to this Microsoft TechNet article for an example: http://technet.microsoft.com/en-us/library/cc770833.aspx.

13.4 PaymentVault™

- Access to the PaymentVault™ configuration file is maintained by operation-system level user permissions.

14 Maintain Instructional Documentation and Training Programs

14.1 General

This document provides the basis from which all Customers, Resellers, and Integrators learn the prudent practices and recommendations for installing Trevance, CN!Express, and PaymentVault in a PCI compliant manner.

Customers, Resellers, and Integrators should maintain their own, internal PCI compliance training for their personnel to ensure they are familiar with the PCI-compliance aspects of running Trevance®, CN!Express®, and PaymentVault™.

Additional phone training is available upon request. Please contact support at: support@AuricSystems.com or 603.924.6079

Part V

Appendices

A Frequently Asked Questions

A.1 Frequently Asked Questions

Question 1 *How do I install and run Trevance® securely?*

Trevance® is compliant with Visa's Payment Application Best Practices standard. See the *Payment Application Best Practices Secure Implementation Guide for Trevance®* document for details. (For information on accessing this document, see Chapter 1.)

Question 2 *Are user accounts designed for application access or individual access to Trevance® ?*

When you configure Users, you decide whether the user is an individual or web application. Most of the accounts are used for human access to the application through the Trevance® Console (TrevCon). The console allows users to configure and monitor transaction processing. Each time you configure a user, you decide what tasks the user can perform.

User accounts can also be used for access through the web. Trevance® installs with one default web-accessible account (WEB). You can establish additional accounts if you want to track the source of a transaction; if you have multiple feeds into the system, you can set up multiple user IDs.

Question 3 *Is Trevance® supposed to have direct access with the Internet?*

No. You must use Trevance® on a non-public network in a secure environment.

Question 4 *Does Trevance® submit any error trapping codes to the front-end application? For example, suppose the front-end application submits a file to Trevance® but the processing service doesn't respond?*

Trevance® always does its best to transmit all transactions from a batch file to the processing service regardless of format errors (although these are flagged in a warning file). Some processing services (such as Chase Paymentech Solutions) don't return any response if the batch is held. Instead, you receive a phone call. Other processing services do send reject or batch hold messages. For more details, see "Part II. Your Processing Service," starting on page 193.

Real-time web interface transactions provide a local response code (ASI Response). So in the example in the question, Trevance® would return an ASI Response of 500 with the text "Authorization Request Timed Out Waiting for Processor Response." The ASI response code returned by the real-time authorization interface (as of May 2004) are:

Table A.1: ASI Response Codes

Authorization	*Meaning*
100	Approved
200	Declined
300	Processor reject

Continued on next page

Table A.1 – *Continued from previous page*

Authorization	*Meaning*
301	Local reject on user/password
302	Local Reject
303	Processor unknown response
304	Error parsing processor response
400	Not submitted
401	Terminated before request submitted
500	Submitted not returned
501	Terminated before response returned

If you POST a request to the web interface and the web interface is not enabled, or some other condition prevents Trevance® from replying to the POST, you'll receive an HTTP error message.

The processing service holds on to transaction data for 20 seconds and can respond up to that time, even if there's a disconnect and reconnect. Therefore, Trevance® times out after 30 seconds.

Question 5 *How does the front-end application know that Trevance® has received a response from the processing service (for example, an approval or decline)?*

For batch transactions, you receive an output file showing the responses.

For web interface transactions, you receive a text string with response codes.

Auric Systems International recommends that you configure transactions to include the LastActionSucceeded field. This field will contain a 1 if the transaction was processed.

Question 6 *How does Trevance® resubmit transactions?*

Trevance® does not automatically resubmit transactions. The application that originally sent the transaction has to re-send it to Trevance® .

Question 7 *Can the real-time monitor and chart display historic data?*

Data is currently available only for the current day. The "day" starts at midnight.

Question 8 *When Trevance® is upgraded from one revision to the next, how is the data maintained in the historical database?*

To update Trevance®, Auric Systems International provides an update DLL and a small database of changes. During startup, Trevance® checks the database version in the small database against the current "live" database. Wherever the small database information is newer, Trevance® applies a set of SQL patches to the "live" database. Thus, the data in the historical database is not replaced.

Question 9 *What files does Trevance® automatically remove, copy, move, rename, or delete?*

Depending on how your configure your real-time and batch import, Trevance® either deletes the imported file or saves it and changes the extension to .DNE, immediately after the file is successfully loaded into the Trevance® data base. On export, files are written with a unique extension and then renamed to the proper extension (.EXP) when all the data is written. This process allows Trevance® to communicate with some 4GL languages that can't specify exclusive read/write access to files. Those are the only cases when Trevance® changes or deletes a file.

Question 10 *Is there any way to directly access the underlying SQL database engine and tables?*

No. Trevance® uses an embedded database that allows only single application access. The activity log can be periodically exported and then loaded into Excel, Access, Oracle, or other programs for further reporting and analysis.

B Troubleshooting Trevance®

If you need to contact Auric Systems International, please:

- Copy down any error messages you received and keep notes on what happened before and after the trouble started.
- Generate, copy, and print your latest configuration report (click on Help, then Configuration Report)
- Have your serial number handy. When you purchased Trevance® over the Internet, the serial number and activation key were e-mailed to you. (You can also find them under the Help menu as explained below.)

This information will help us solve your problem quickly.

To contact technical support for Trevance® :

Phone:	603-924-6079
E-mail:	support@AuricSystems.com
Web Site:	http://www.AuricSystems.com

You can find your serial number and activation key under the Help menu:

1. Click on Help.
2. Click on About.
3. Scroll down to Serial Number and then Activation Key.

4. Write down the numbers.
5. Click on

to leave the Help menu.

Your problem might involve the external application or your processing service. Contact your processing service directly.

C Secure File Deletion

C.1 General

Trevance® and CN!Express® support secure file deletion methods. Normally, files deleted using the standard services provided by the operating system do not erase the actual data in the file. Files deleted this way can be easily recovered using software "undelete" tools. Even files that have been overwritten can sometimes be recovered using additional hardware and sophisticated forensic techniques.

Trevance® and CN!Express® offer three deletion choices ranging from the quick (but not secure) standard operating system delete to a multi-pass secure deletion:

- Quick Delete
- One-Pass Overwrite and Delete
- Multi-Pass Overwrite and Delete

Because the multi-pass secure deletion requires 35 write passes over the file, some sites may determine this consumes too much time or causes too much hard disk activity and interferes with other services. To address this, Trevance® and CN!Express® provide a one-pass secure delete that simply overwrites the file data with 0's before deleting.

C.1.1 Quick Delete

- Uses standard operating system calls.
- Doesn't overwrite any of the file (typically only the directory entry is updated) and so is very fast.
- File data is easily recovered if this option is used.

C.1.2 One-Pass Overwrite

- File is overwritten with a single pass of binary zeros.
- This makes it difficult to recover the file using "undelete" tools.
- Theorectically, the file data might still be recoverable using sophisticated forensic tools.

C.1.3 Multi-Pass Overwrite and Delete

- Overwrites file data with 35 passes using various data patterns.
- The 35 overwrite patterns, though possibly considered excessive for modern drives, is specifically designed to make data recovery extremely difficult.
- The pattern was developed by Peter Gutmann, and is often the pattern used by secure deletion utilities.
- Gutmann's paper describing the pattern can be found at: http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html.

C.2 Trevance®

Secure delete is primarily intended for batch import files, but Trevance® also applies the secure delete option to any external file that it handles that may contain sensitive information, including temporary encryption files created during the upload and download process.

When Trevance® is uninstalled, the secure delete process is used to delete all configuration and data files that might contain sensitive information. Note that log files are not removed during the uninstall process.

C.3 CN!Express®

Secure deletion applies to all imported files (both single- and multi-transactions).

When CN!Express® is uninstalled, the secure delete process is used to delete all configuration and data files that might contain sensitive information. Note that log files are not removed during the uninstall process.

C.4 PaymentVault™

PaymentVault™ does not have import files.

D Error and Event Messages

Trevance® System Errors that may be reported by E-Mail. These messages are descriptive of the issue that Trevance has encountered.

D.1 General Notes

- When making Auric Systems International Technical Support aware of a situation that cannot be resolved by the merchants internal IT staff, please provide Trevance® Logs (found in the Trevance Log Directory). Each section below has suggested Trevance® logs which may assist in expedited resolutions.
- Auric Support email: Support@AuricSystems.com or call Auric Systems International support at 603-924-6079.
- Many of the errors listed below will never be encountered during normal operations.
- Socket errors are reported only once per connection incident.
- A maximum of 20 batch generation errors are reported per batch.
- Exceptions may generate additional messages that include the exception text.
- Additional messages may be logged during server configuration.
- In the Events section messages (below), %s is a placeholder for an additional string that is usually further details on the type of error and %d is a placeholder for a number.

D.2 Trevance® Logs

These Trevance® logs may be useful for evaluating errors. Trevance® log files never contain sensitive cardholder information (the transactions have been sanitized). However, they may still contain sensitive personal information such as addresses, phone numbers, and emails.

A new log file is created each day. The actual name of the log file will contain the date as well as the base name (e.g., trevance_20110914.log).

For PCI compliance, you must monitor and store your logs in a centralized location. The Trevance® logs to be transported to the centralized location are located in the TrevanceData folder.

Trevance Log: Contains the general activity of the Trevance® application/service.

Exception Log: Contains server related and Trevance® inner working events (exceptions are not always indicative of a problem occurring).

Socket Log: Contains Real-Time communication events with the Payment Processor.

Web Log: Contains Real-Time communication events with Merchant's business environment (communications sent to and from Trevance® via the web interface).

Batch Upload/Download Logs: Contains information on Batch upload and download files.

Batch Protocol Logs: Contains information at Batch Communication level with payment processor.

Windows System Event Logs: These logs are located under the Administrator Tools >Event Viewer. Corresponding Errors events logs may be useful for some resolutions.

D.3 Configuration Report

The configuration report provides information on how Trevance® is configured in the merchant's business environment. For the purposes of technical support, Auric Systems International cannot use the .xml version of this report. The following way of obtaining the configuration report is sanitized of sensitive information. Run (Trevance® Administrative Console>Help >Configuration Report). The report will be copied to the clipboard and can be pasted into other documents or email

D.4 Events

D.4.1 Server Management Events

Message: Automatic Password Change Error: %s
Expanded Information: Some Trevance® versions support processor-specific password management requirements and automate the password change process. This message occurs when there is a problem with the automated password change.
Suggested Action: Review with your Payment Processor for a possible Password Reset. See Trevance® manual or Doc's directory for additional Password Management information.

Message: Can't Send E-Mail Notification Because E-Mail Settings Are Incomplete.
Expanded Information: Trevance® Can't Send E-Mail Notification Because E-Mail Settings Are Incomplete.
Suggested Action: Review and complete the email settings in Trevance® (Trevance Menu: Configure >Email Notification)

Message: Console Port Error: %s
Expanded Information: Trevance® Console Port is configured incorrectly,
Suggested Action: Review (Trevance Menu: Configure>Set Console Port)

Message: Disabling Web Interface. Correct port error using console.
Expanded Information: Trevance Console Port is configured incorrectly in the Console login dialogue box, (Trevance Console: port)
Suggested Action: Configure Trevance Console Port to correct setting

Message: Error Sending E-Mail Notification: %s
Expanded Information: Trevance could not successfully send an E-mail notification
Suggested Action: Review Email Settings (Trevance Menu: Configure >Email Notification) or Review Email provider status

Message: Error connecting to Trevance database.
Expanded Information: Trevance is experiencing an issue while connecting to the Trevance database.
Suggested Action: Review if a process (Example: anti-virus application scans) may be preventing Trevance from connecting to the database.

Message: Error saving log information for transaction #%s. Error was '%s'. Please contact Auric Systems technical support.
Expanded Information: Trevance encountered a problem when saving the log information.
Suggested Action: Review disk space, permission or previously open log for log directory.

Message: Fatal Error: %s Shutting Down
Expanded Information: Trevance has encountered a significant problem and is shutting down.
Suggested Action: Review for Hardware, Disk space, or Operating System issues. Contact Auric Technical support: Support@AuricSystems.com Or Call 603-924-6079
Provide Auric support the suggested Trevance Logs below

Message: Trevance is already running. Please pause and exit Trevance and try starting the service again.
Expanded Information: Trevance has encountered another instance of Trevance previously running on the current server.
Suggested Action: Review for another instance running as an application or a Service.

Message: The Trevance server has become unstable.
Expanded Information: Trevance has encountered a significant problem and is shutting down.
Suggested Action: Review for Hardware, Disk space, or Operating System issues. Contact Auric Technical support. Support@AuricSystems.com Or Call 603-924-6079. Provide Auric support the suggested Trevance logs below.

Message: The database includes items that are not supported by this version of Trevance. Trevance will PAUSE. Please contact Auric Systems Technical Support.
Expanded Information: Trevance found transactions in the database that are not compatible with this version or are not supported by the license.
Suggested Action: Contact Auric Technical support: Support@AuricSystems.com Or Call 603-924-6079. Provide Auric support the suggested Trevance logs below.

Message - Unable to resume server; The database includes items that are not supported by this version of Trevance. Please contact Auric Systems Technical Support.
Expanded Information: Trevance found transactions in the database that are not compatible with this version or are not supported by the license.
Suggested Actions: Contact Auric Systems International Technical Support and Provide These Suggested Logs with Server Management Events.

Message: Unrecoverable timeout error on HTTP shutdown. Please shutdown the server and restart.
Expanded Information: During an attempted pause, Trevance encountered a timeout while shutting down the HTTP web interface. Shutdown the server and restart.
Suggested Action: Shutdown the server and restart.

Message: Information: Running on Primary

$$orSecondary$$

(ip-address

$$SSL$$

:port) **Expanded Information:** Message is generated during each daily maintenance. Allows monitoring of which connection (primary/secondary) is currently active.

Message: Warning: Timeout on primary socket: primary socket automatically changed to

$$ipaddress$$

:socket. **Expanded Information:** Message occurs when a time-out or connection error occurs and primary socket is no longer able to communicate with the payment processor. **Suggested Action:** You should monitor for this message and explore why the switch-over occurred. It could be indicative of pending hardware or communications failures in the environment.

Message: Information: Switching from Primary (ip-address) to Secondary (ip address). **Expanded Information:** Message occurs when Primary is unable to connect but Secondary remains active. **Suggested Action:** You should monitor for this message and explore why the switch-over occurred. It could be indicative of pending hardware or communications failures in the environment.

D.4.1.1 Provide These Suggested Logs with Server Management Events

- Trevance Log
- Exception Log
- Socket Log
- Web Log

- Batch Upload/Download Logs
- Batch Protocol Log
- Configuration Report
- Windows event logs

D.4.2 Error Reading or Writing Events

Message: Error writing to batch log. Duplicate batch.
Expanded Information: Trevance can't update the batch log while attempting to export a batch. Most likely cause is improper recovery from recovery log (for example, saving a recovery log, exporting a batch, and then recovering from the out-of-date recovery log and exporting it again).
Suggested Action: Use non-out-of-date recovery log in recovery process

Message: Error writing to log file '%s'.
Expanded Information: Trevance could not successfully write to a log file.
Suggested Action: Review for Open log, Disk space, or other application that may have the log open.

Message: Error: Can't access directory "%s".
Expanded Information: Trevance could not successfully access a directory.
Suggested Action: Review Directory location and status, Disk space, or other reasons for directory access failure.

Suggested Trevance logs to provide to Auric Support for read/write error events are:
Trevance Log
Exception Log

Socket Log
Web Log
Batch Upload/Download Logs
Batch Protocol Log
Configuration Report:
Windows System Event logs

D.4.3 Real-Time Events

Note: Socket connection errors follow this template:

Error:Error connecting to Authorization Host <host:port>
(<PRIMARY—SECONDARY >SOCKET): 'Socket Error # <error>
<error >'. Retrying...

This should be considered a serious error. The connection should be considered inactive until Trevance logs a matching "connection established" message:

Information:Connection established to Authorization Host <host:port>
(<PRIMARY—SECONDARY>SOCKET).

If both the primary and secondary connections are inactive, Trevance will respond to real- time requests with:

ASIRESP: 400
RESPTEXT: Connection to authorizing host is not active. Unable to complete request.

Any ASIRESP of 400 means that the transaction was not submitted to the processor. It also indicates that there is a serious network issue that should be addressed.

Message: Error building response: '%s'.
Expanded Information: An error occurred while translating the processor response to the response to be returned from the web interface. The message will contain more information about the cause of the error.
Suggested Action: Review message and take appropriate action.

Message: Error connecting to Authorization Host %s%s:'%s'. Retrying...
Expanded Information: Trevance could not successfully connect to the Authorization Host (Payment Processor).
Suggested Action: Review for Networking issue. Contact Payment Processor to troubleshoot event cause.

Message: Error dequeueing auth request. (Error #%d). Please contact technical support.
Expanded Information: Trevance encountered an error while reading a transaction from an internal queue.
Suggested Action: Please provide the message and error number to Auric Technical support. Support@AuricSystems.com Or Call 603-924-6079. Provide Auric support the Trevance logs suggested below.

Message: Error in socket interface: %s.
Expanded Information: An unexpected error occurred in sending or receiving real-time transactions through the socket. The message will contain more information about the cause of the error.

Suggested Action: Review message and take appropriate action.
Message: Error saving capture information for authorized transaction #%s (submitted as Auth-Capture). Error was '%s'. Please contact Auric Systems technical support.

Expanded Information: Trevance received a "Sale" transaction. Internally, this is handled as a separate authorization to the Payment Processor, followed by a batch settlement. The authorization succeeded, but Trevance failed to save that successful Auth for the Batch Settlement Process (CN-4250 Auto Settlement functionality).
Suggested Action: Contact Auric Technical support. Support@AuricSystems.com Or Call 603-924-6079.
Provide Auric support the Trevance Logs suggested below.

Message: Error saving qualification information for authorized transaction #%s. Error was '%s'. Please contact Auric Systems technical support.
Expanded Information: Trevance saves qualification information for authorized transactions (if required) so that it can supply the information to the processor during capture (deposit). There was an error storing that qualification information to the database.
Suggested Action: Contact Auric Technical support.
Support@AuricSystems.com Or Call 603-924-6079. Provide Auric support the Trevance Logs suggested below.

Message: Error updating summary information for transaction #%'s. Error was '%s'. Please contact Auric Systems technical support.
Expanded Information: There was an error updating the transaction information displayed in Trevance Console.
Suggested Action: Contact Auric Technical support. Support@AuricSystems.com Or Call 603-924-6079. Provide Auric support the Trevance Logs suggested below.

Message: Error parsing returned transaction: %s
Expanded Information: The response returned from the payment processor was not in the expected format. Trevance may have encountered invalid characters that prevent it from correctly parsing the transaction information.
Suggested Action: Review the Web and Socket logs for invalid

characters.

Message: HTTPS server startup failed; reverting to HTTP.
Expanded Information: Trevance did not successfully start up an HTTPS connection.
Suggested Action: Review for proper HTTPS configuration and Certificates (Trevance Administrative Console>Configure>Real-Time Interface>HTTPS Configuration)

Message: HTTPS server startup failed; reverting to HTTP. Error was: OpenSSL DLLs not installed in Trevance Server directory.
Expanded Information: Trevance did not successfully start up an HTTPS connection.
Suggested Action: Review for proper HTTPS configuration and Certificates (Trevance Administrative Console>Configure>Real-Time Interface>HTTPS Configuration)

Message: Late Authorization Response received for item #%'s; authorization already reported failed with No Response.
Full Response was [%s].
Expanded Information: Trevance received the response to a Real-Time transaction >40 seconds from the time the request was sent. The transaction was already reported failed with no response. This message can be used to help determine whether or not the authorization succeeded.
Suggested Action: determine whether or not the authorization succeeded.

Message: Socket Log Error: Unrecognized format code %s.
Expanded Information: Trevance received an unrecognized format code in the processor response, so does not know the length of the corresponding segment. Therefore, the socket log may be inaccurate.

Suggested Action: Contact Auric Technical support, Support@AuricSystems.com Or Call 603-924-6079. Provide Auric support with the text of the error message.

Message: Terminating Thread #%d
Expanded Information: May occur during pause or shutdown if an individual thread was unresponsive and needed to be terminated.
Suggested Action: None

Message: Timeout error waiting for active HTTP threads to complete. Clearing DB request queue.
Expanded Information: May occur during pause and shutdown if web-servicing threads become unresponsive.
Suggested Action: None

Message: Web Interface %s Server Error: %s
Expanded Information: An error occurred while attempting to start the web interface.
Suggested Action: Review the Web interface settings (Trevance Administrative Console>Configure>Real-Time Interface)

Message: Web Interface %s Server not started.
Expanded Information: The Trevance CN-4200, and CN-4250 feature a Web Interface for Real-Time Transactions. Trevance indicates that the web interface did not start.
Suggested Action: Review the Web interface settings (Trevance Administrative Console>Configure>Real-Time Interface)

Suggested Trevance logs to provide to Auric Support for
Real-Time events are:
Trevance Log
Exception Log
Socket Log
Web Log

D.4.4 Batch Events

Message: Batch conversion failed: %s
Expanded Information: There was an error in converting a batch to
payment-processor specific format. The error message should contain more information about the cause of the error.
Suggested Action: Review error message and take appropriate action

Message: Exported batch file %s contains %'d items that failed to settle. Please review exported file.
Expanded Information: Trevance indicates that the Batch contains items that failed to settle or deposit (settlements are expected to succeed, so
failing to settle is an error).
Suggested Action: Review the exported file.

Message: No Response Received for Batch After 1 Hour: %s.
Expanded Information: Batches should never take more than an hour to return. Message indicates batch is probably on hold at payment processor.
Suggested Action: Contact payment processor.

Message: Error loading import/export template %s: %'s
Expanded Information: Trevance has encountered a problem loading the import/export template at startup. This should not occur unless there is an installation error.
Suggested Action: Review Installation

Message: Export FAILED for Processor File '%s' with Error: %'s
Expanded Information: Trevance received an Batch Response file from the processor but could not export it properly.
Suggested Action: Review specifics indicated in Error message and
correct

Message: File download error: %s
Expanded Information: Trevance experienced a problem retrieving a Batch file from the processor.
Suggested Action: Review the Batch Protocol Log of the event and/or contact your Payment Processor for assistance.

Message: File upload error: %s
Expanded Information: Trevance experienced a problem uploading a Batch file to the processor.
Suggested Action: Review the Batch Protocol Log of the event and/or contact your Payment Processor.

Message: Import FAILED for %s with Error: %'s
Expanded Information: Trevance detected a File in the Batch Import folder but could not import it.
Suggested Action: Review the File for formatting issues

Message: Internal Error on ID Queue Write. [Error #%d].
Expanded Information: An internal error occurred.

Suggested Action: Please provide the message and error number to Auric Technical support. Support@AuricSystems.com
Or Call 603-924-6079.
Provide Auric support the Trevance Logs suggested below.

Message: Internal Error on Message Queue Read. [Error #%d].
Expanded Information: An internal error occurred.
Suggested Action: Please provide the message and error number to
Auric Technical support.
Support@AuricSystems.com Or Call 603-924-6079.
Provide Auric support the Trevance Logs suggested below.

Message: PUT Exception: %s
Expanded Information: Trevance has encountered a problem with the Batch interface for the Payment Processor, and was unable to upload a file.
Suggested Action: Review the Batch Protocol Log and Processor
Settings for correct Batch interface settings (Trevance Administrative
Console>Configure>Processor Settings>Server Info>Batch)

Message: SFTP Error: %s.
Expanded Information: Trevance has encountered a problem with the Batch interface for the Payment Processor.
Suggested Action: Review the Batch Protocol Log and Processor
Settings for correct Batch interface settings(Trevance Administrative
Console Configure>Processor Settings>Server Info>Batch)

Message: Watchdog: Batch thread error detected
Expanded Information: The batch processing thread has become
unresponsive, and Trevance will attempt to automatically restart it.
Suggested Action: Monitor the server for further errors and restart
Trevance if necessary.

Message: Watchdog: Batch thread restart failed: %s
Expanded Information: The batch processing thread has become
unresponsive, and could not be restarted.
Suggested Action: Please restart Trevance as soon as possible.

Message: Zip Password Error: Can't extract file %s from archive. Please contact technical support.
Expanded Information: Trevance supports various password protocol with payment processors review (Trevance Administrative Console>Configure
>Processor Settings>Server Info>Batch)
Suggested Action: Review password protocol with your payment processor

Suggested Trevance logs to provide to Auric Support for batch events are:
Trevance Log
Exception Log
Batch Upload/Download Logs
Batch Protocol Log
Configuration Report

D.4.5 Method of Payment Events

Message: Internal Error: Real Time DB Queue Function: Invalid Action: Partial reversal sent as specified, but partial reversal supported for Visa only.
Expanded Information: Trevance supports rules specific to Methods of Payments (MOP)
Suggested Action: Review for specific MOP and correct.

Message: Invalid Action: Reversal sent as specified, but reversal supported for Visa, American Express only.
Expanded Information: Trevance supports rules specific to Methods of Payments (MOP)
Suggested Action: Review for specific MOP and correct.

Suggested Trevance logs to provide to Auric Support method of payment events are:
Trevance Log
Exception Log
Socket Log
Web Log
Batch Upload/Download Logs
Batch Protocol Log
Configuration Report

D.4.6 Auric Cipher Engine™ (ACE) Events

Message: ACE Decrypt Error: %s
Expanded Information: Trevance can support Custom Encryption/ Decryption through the ACE interface
Suggested Action: Review the ACE server setting (Trevance Administrative Console>Configure>Options >Security>ACE) and review Merchants Internal Encryption/ Decryption service for proper operation

Message: ACE Encrypt Error: %s
Expanded Information: Trevance can support Custom Encryption/ Decryption through the ACE interface
Suggested Action: Review the ACE server setting (Trevance Administrative Console>Configure>Options >Security>ACE) and review Merchants Internal Encryption/ Decryption service for proper operation

Message: Error communicating with ACE server: %s
Expanded Information: Trevance can support Custom Encryption/ Decryption through the ACE interface
Suggested Action: Review the ACE server setting (Trevance Administrative Console>Configure>Options >Security>ACE)

and review Merchants Internal Encryption/ Decryption service for proper operation

Suggested Trevance logs to provide to Auric Support ACE events are:
Trevance Log
Exception Log
Configuration Report

D.4.7 PaymentVault™ Events

Message: Duplicate UTID Generated: %s.
Expanded Information: Trevance has generated a duplicate UTID
(this is extremely unlikely to occur).
Suggested Action: Review the transaction and resubmit it for a unique UTID

Message: PaymentVault™ Lookup Error: %s
Expanded Information: Trevance attempted to lookup a UTID value, but encountered a problem
Suggested Action: Review PaymentVault™ Location (Trevance Administrative Console>Configure>Options>PaymentVault™) Review PaymentVault™ Server for Operational Status. Review PaymentVault™ Logs for indication of problem

Message: PaymentVault™ Migration: %s
Expanded Information: Trevance attempted to migrate UTID values to PaymentVault™ but encountered a problem
Suggested Action: Review PaymentVault™ Location (Trevance Administrative Console>Configure>Options>PaymentVault™) Review PaymentVault™ Server for Operational Status. Review PaymentVault™ Logs for indication of problem

Message: PaymentVault™ migration had errors. Please shutdown the
Trevance server and restart.
Expanded Information: Trevance attempted to migrate UTID values to PaymentVault™ but encountered a problem.
Please restart the Trevance server.
Suggested Action: Review PaymentVault™ Location (Trevance Administrative Console>Configure>Options>PaymentVault™) Review PaymentVault™ Server for Operational Status. Review PaymentVault™ Logs for indication of problem. Please shutdown the Trevance server and restart.

Message: UTID PaymentVault™ Migration Error: %s
Expanded Information: Trevance attempted to migrate UTID values to PaymentVault™ but encountered a problem
Suggested Action: Review PaymentVault™ Location (Trevance Administrative Console >Configure>Options>PaymentVault™) Review PaymentVault™ Server for Operational Status.
Review PaymentVault™ Logs for indication of problem

Suggested Trevance logs to provide to Auric Support for PaymentVault™ events are:
Trevance Log
Exception Log
PaymentVault™ Logs (Found on the PaymentVault™ Server)(PV.log)

E Level III Transactions

This chapter describes how Trevance® handles Level III transactions. Level III is currently supported only by Chase Paymentech Solutions.

E.1 Purchase Card Line Items

Trevance® supports purchase card (level III) for MasterCard and Visa. Level III is typically used in a business-to-business environment and provides for the inclusion of order and line item information with purchase card settlement transactions.

Level III information is accepted only through theTrevance® batch interface. You don't need to provide level III-specific information authorization time, only at settlement/capture time.

Table E.1: Level III Specific Fields

Field	*Description*	*MC/Visa*	*Refund*
FREIGHT	Freight paid for order	M, V	Expiration Date
DUTY	Duty paid for order	M, V	
SHIPCTRY	Ship-to country	M, V	
SHIPZCPC	Ship-to Zip/Postal Code	M, V	
SFRMZCPC	Ship-from Zip/Postal Code	M, V	

Continued on next page

Table E.1 – *Continued from previous page*

Field	*Description*	*MC/Visa*	*Refund*
DISC	Discount Amount on Entire Order	V	
VATRATE	VAT/Tax Rate	V	
VATAMT	VAT/Tax Paid on Order	V	
ALTTXID	Alternate Tax ID	M	
ALTTXAMT	Alternate Tax Amount	M, V	

None of these fields are required for level III, but they can help improve your interchange rate (processing fee). Please contact your processing service's representative to determine which, if any, of these fields you should import.

E.2 Level III Line-Item Records

The level III specification allows merchants to provide specific line-item information to MasterCard and Visa. These line item entries appear on the customer's statement.

In the Trevance® batch import file, level III line items (called L3 line items in the rest of this document) are entered one per line immediately after the import line that contains the primary transaction information. The characters ∼ L3 ∼ at the start of a line indicate L3 line items.

Here is a sample L3 line item:

∼ L3∼ CAP,PROMO CAP-2982 50 EA 4.99 10.00 0.05 12.48 251.48 CLOTHING Y MA Y PER STUART

L3 line items contain the same delimiter as the standard transaction lines–typically a tab or comma. The example shown above has a tab character between each field. Optionally, you can also surround each field with double quotes(“ ”). If you use double quotes, you should also double quote the leading tag. Use “∼L3∼” instead of just ∼L3∼ at the beginning of the line.

Aside from those options, L3 items use a pre-defined format as described next.

The following table shows the L3 item fields and the order in which they must appear. You’re required to fill in only the fields listed as mandatory. Some fields aren’t used for MasterCard and some aren’t used for Visa.

Table E.2: Line Item Samples

Field Number	*Name*	*Mandatory*	*MC/Visa*	*Description*
1	Tag	Yes	M, V	Literal: ∼L∼
2	L3_DESCRPT	Yes	M, V	Product description
3	L3_PRODCODE	Yes	M, V	Product code
4	L3_QTY	Yes	M, V	Quantity purchased
5	L3_MEASURE	Yes	M, V	Unit of measure (for example, EA)
6	L3_UNITCOST		M, V	Cost per unit

Continued on next page

Table E.2 – *Continued from previous page*

Field Number	*Name*	*Mandatory*	*MC/Visa*	*Description*
7	L3_DISC		M, V	Discount amount
8	L3_TAXRATE		M, V	Tax rate on item
9	L3_TAX		M, V	Tax paid on item
10	L3_ITEMAMT	Yes	M, V	Item total amount
11	L3_COMDCODE		V	Commodity code
12	L3_INCLTAX		M	Total contains tax
13	L3_TAXTYPE		M	Tax Type
14	L3_ISDISC		M	Discount indicator
15	L3_COMMENT			Local Comment

E.3 Importing

The following table describes the information that can be imported into each field and the maximum length of that field. Do not pad the field with 0s or blanks to extend it to the maximum length.

Table E.3: Importing

Field Number	*Name*	*Type*	*Example*	*Description*
1	Tag	Literal: ~L3~	~L3~	
2	L3_DESCRPT	A/N [35] (MC) A/N [26] (VI)	CAP, PROMO	General description of the purchased product
3	L3_PRODCODE	A/N[12]	CAP-2982	Product code
4	L3_QTY	N[4]	50	How many (or much) purchased. Cannot be 0. Must be whole number.
5	L3_MEASURE	A/N[12]	EA	Free form field. Paymentech has compiled a list of suggested standard measures which is available on the web at http://www.AuricSystems.com/level_3_measures
6	L3_UNITCOST	N[12]1(VI)	4.99	Cost for this line item
7	L3_DISC	N[12]1	10.00	Amount of discount applied to this line item.

Continued on next page

Table E.3 – *Continued from previous page*

Field Number	*Name*	*Type*	*Example*	*Description*
8	L3_TAXRATE	N[4]	0.05	Tax rate on item
9	L3_TAX	N[12]1	12.48	Tax amount for this item
10	L3_ITEMAMT	N[12]1	251.48	The amount for this line item
11	L3_COMDCODE	A/N[12]	CLOTHING	Commodity code used to classify the item purchased
12	L3_INCLTAX	Y/N	Y	Indicates whether tax amount is included in item amount. Y if item amount includes tax amount. N if item amount does not include tax amount. Paymentech calls this field the "gross/net indicator"
13	L3_TAXTYPE	A/N[4]	MA	Text description of the type of tax. MA (Massachusetts)
14	L3_ISDISC	Y/N	Y	Is the amount discounted? Y if discounted. Otherwise, N
15	L3_COMMENT	A/N[20]	PER STUART	Available for internal comments. Not sent to Paymentech

NOTES:
1Maximum of 12 digits for Visa, but only 9 digits for MasterCard

Trevance® supports up to 98 L3 items. The 99th line item (and beyond) is not imported. The excess records are sent to the

WARNING folder.

The order in which L3 items are imported is significant. Items are sent in the same order in which they are imported.

E.4 Exporting

L3 line items can be exported as well as imported. When exported, they appear immediately following the transaction that includes the order information.

Exporting is controlled by the EXPORT LEVEL 3 DETAIL RECORDS checkbox in the EXPORT CONFIGURATION dialog. The delimiter and optional quotes are controlled by the main export settings.

F Contact Auric Systems International Technical Support

You can contact Auric Systems International technical support at:

- support@AuricSystems.com
- 603.924.6079